TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

INTERNETOVÉHO BANKOVNICTVÍ - PŘEDNOSTI A HROZBY

Bakalářská práce

Studijní program: B6209 – Systémové inženýrství a informatika
Studijní obor: 6209R021 – Manažerská informatika

Autor práce: **Vladimír Škarda**
Vedoucí práce: Ing. Zbyněk Hubínka

Liberec 2014

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Economics

THE ISSUE OF INTERNET BANKING

Bachelor thesis

Study programme: B6209 – System Engineering and Informatics
Study branch: 6209R021 – Managerial Informatics

Author: **Vladimír Škarda**
Supervisor: Ing. Zbyněk Hubínka

Liberec 2014

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vladimír Škarda**
Osobní číslo:	**E12000486**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Manažerská informatika**
Název tématu:	**Internetového bankovnictví - přednosti a hrozby**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

1. Základní charakteristika e-banking
2. Současné technologie
3. Technologie zabezpečení
4. SWOT analýza
5. Doporučení pro minimalizaci možných ohrožení (pro různé skupiny uživatelů)

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 normostran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

MATYÁŠ, V. a J. KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. 1. vyd. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.
PŘÁDKA, M. Elektronické bankovnictví: [rady a tipy]. 1. vyd. Praha: Computer Press, 2000. ISBN 80-7226-328-5.
KALABIS, Z. Základy bankovnictví: bankovní obchody, služby, operace a rizika. 1. vyd. Brno: BizBooks, 2012. ISBN 978-80-265-0001-8.
DOSTÁLEK, L. Velký průvodce protokoly TCP/IP: bezpečnost. 1. vyd. Praha: Computer Press, 2001. ISBN 80-7226-513-X.
Elektronická databáze článků ProQuest (knihovna.tul.cz).

Vedoucí bakalářské práce: **Ing. Zbyněk Hubínka**
Katedra informatiky

Konzultant bakalářské práce: **Ing. Petr Rozmajzl**
Katedra informatiky

Datum zadání bakalářské práce: **30. října 2013**

Termín odevzdání bakalářské práce: **7. května 2014**

doc. Ing. Miroslav Žižka, Ph.D.
děkan

Technická univerzita v Liberci
Ekonomická fakulta
L.S.

doc. Ing. Jan Skrbek, Dr.
vedoucí katedry

V Liberci dne 30. října 2013

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Poděkování

Tímto bych chtěl poděkovat všem, kteří mi svým jednáním či svými myšlenkami pomohli k uskutečnění této bakalářské práce. Panu Ing. Zbyňku Hubínkovi za vedení mé bakalářské práce, mé rodině, mé přítelkyni, mým přátelům a pedagogům za podporu během celého studia.

Anotace

Bakalářská práce rozebírá problematiku elektronického bankovnictví a zaměřuje se především na bezpečnost a technologii zabezpečení. Teoretická část mé práce popisuje základní charakteristiky Internetového bankovnictví, typy komunikací mezi bankou a klientem a současně využívané technologie. Dále se detailně zaobírá technologií zabezpečení, zejména bezpečnostními certifikáty, protokoly, šifrováním, hesly, přihlašováním a ochranou citlivých dat. V praktické části tato práce porovnává čtyři Internetová bankovnictví různých bank na českém trhu. Rozebírá především bezpečnost a technologie zabezpečení, ale i možnosti jednotlivých bankovnictví, uživatelské rozhraní až po celkový vzhled. V neposlední části této práce jsou uvedeny výsledky testů Internetových bankovnictví vybraných bank a anonymní anketa, která je zaměřena na využívání Internetového bankovnictví. Na závěr jsou uvedeny rady a tipy vyplývající z této práce pro různé skupiny uživatelů.

Klíčová slova

Elektronické bankovnictví, bezpečnost, zabezpečení, klient, server, certifikát, protokol, služba.

Annotation

Bachelor thesis analyzes the electronic banking and focuses primarily on safety and security technology. The theoretical part of the thesis describes the basic characteristics of Internet banking, types of communications between the bank and the client and the current uses of technology. Further detail deals with security technologies, particularly security certificates, protocols, encryption, passwords, login, and protection of sensitive data. In the practical part of this work compares four different Internet banking of banks on the Czech market. It discusses in particular about the safety and security technologies, but also the possibilities of bank user interface and overall look. Last but not least part of this work presents the results of tests of Internet banking of banks and anonymous questionnaire, which focuses on the uses of internet banking. At the end stated the recommendations for different groups of users based on this thesis.

Keywords

Electronic banking, safety, security, client, server, certificate, protocol, service.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

BÚ – běžný účet

IB – internetové bankovnictví

Úvod

Internetové bankovnictví je služba, kterou v současné době využívá stále více vlastníků bankovních účtů. S touto službou jsou spojeny nejen výhody, ale i bezpečnostní rizika, která mohou vést nejen ke ztrátě citlivých informací, ale i k odcizení finančních prostředků.

Cílem mé bakalářské práce je poukázat na přednosti a hrozby související s Internetovým bankovnictvím, především na základě zabezpečení, ale i uživatelského prostředí a produktů, které Internetové bankovnictví poskytuje.

Bakalářská práce je rozdělena do pěti částí. V první části jsem se zaměřil na obecné informace a samotnou podstatu internetového bankovnictví. Druhá část práce popisuje současné technologie využívané v rámci síťové architektury a popisuje jednotlivé komunikační prvky, jako jsou protokoly a služby. Ve třetí části se zabývám technologií zabezpečení síťové komunikace, do které patří především způsoby přihlašování do Internetového bankovnictví, bezpečnostní protokoly, certifikáty a metodika šifrování. Celá čtvrtá část zahrnuje analýzu vybraných bank především z hlediska zabezpečení poskytovaného Internetového bankovnictví. Do této části je také zahrnuta mnou provedená anonymní anketa, týkající se využívání Internetového bankovnictví. V páté části uvádím doporučení pro minimalizaci možných ohrožení pro různé skupiny uživatelů.

1. Základní charakteristika Internetového bankovnictví

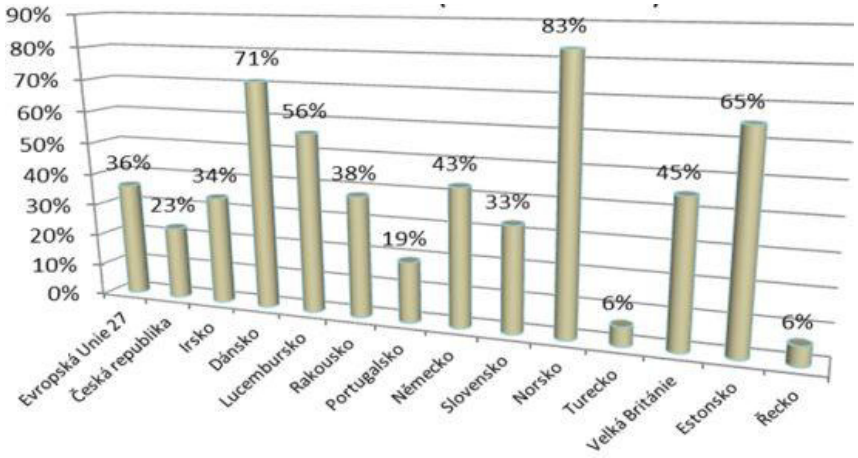
Internetové bankovnictví je služba, kterou poskytuje banka, spadá do elektronického bankovnictví mezi Mobilní bankovnictví (Smart banking), Telebanking, Home banking, GSM banking a Wap banking.

Internetové bankovnictví je jedna z nejrozšířenějších a nejsnazších metod komunikace klienta s bankou v posledních letech. Internetové bankovnictví umožňuje provádět bankovní operace z jakéhokoli počítače připojeného k internetu pomocí webového rozhraní. Téměř každá banka již Internetové bankovnictví poskytuje a nabízí prakticky všechny funkce jako klasická bankovní pobočka. Prostřednictvím Internetového bankovnictví je možné zadávat příkazy k úhradě, trvalé i jednorázové, zjistit zůstatek na účtu, zobrazit historii transakcí, zakládat inkasa a další služby. Některé banky nabízí např.: přímé investice do různých fondů, přehledy spotřebitelských úvěrů, hypoték, dobití předplacené karty mobilního operátora. Nejdůležitějším prvkem celého systému komunikace mezi bankou a klientem je zabezpečení klientovy identity, jeho osobních údajů a transakcí, protože webové rozhraní pracuje s jeho penězi. [1]

1.1. Grafy, využití a užívání Internetového bankovnictví ve světě

Dle průzkumu z roku 2010, o kterém píše portál Firemní finance.cz, je situace na Evropském trhu, díky stále zvyšujícímu se šíření internetu a zvyšujícímu se počtu bank nabízejících Internetové bankovnictví, velice různorodá.

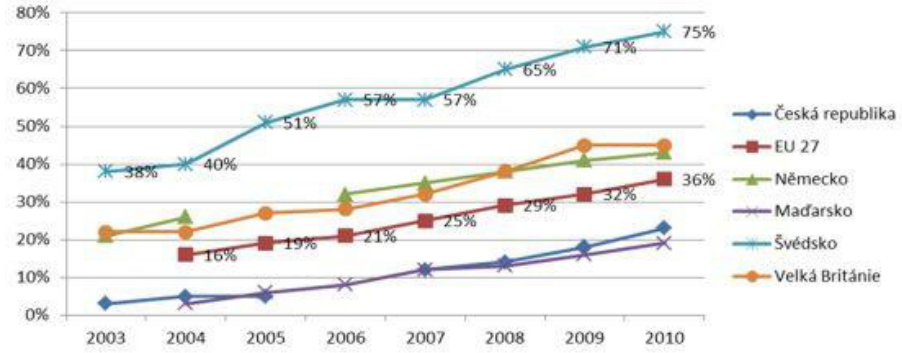
Graf 1 – Využití internetového bankovnictví ve světě



Zdroj: [online]. [cit. 2014-04-07]. Dostupné z: http://jpg.assets-finance-media.cz/newsimg/Grafy_2011/ib_1.jpg

Na následujícím grafu je zcela zřetelný nárůst v užívání internetu pro Internetové bankovnictví od roku 2003 do roku 2010 ve vybraných zemích. Největší nárůst uživatelů Internetového bankovnictví zaznamenává Švédsko. [2]

Graf 2 – Nárůst v užívání internetu pro Internetové bankovnictví ve světě



Zdroj: [online]. [cit. 2014-04-07]. Dostupné z: http://assets-finance-media.cz/newsimg/Grafy_2011/ib_2.jpg

1.2. Jak funguje Internetové bankovnictví

V dnešní době je nejpoužívanějším typem přístupu k Internetovému bankovnictví webové rozhraní, které je označováno jako plnohodnotné. Klient otevře internetovou stránku své banky a přihlásí se, to je prováděno specifickým způsobem dle banky, u které má účet zřízen. Výhodou plnohodnotného přístupu je možnost připojení z jakéhokoli počítače připojeného k internetu nezávisle na instalovaném softwaru.

Druhým typem přístupu k Internetovému bankovnictví je přístup neplnohodnotný. U tohoto způsobu je zapotřebí nainstalovat speciální bezpečnostní software, pomocí kterého jsou generovány digitální certifikáty a digitální podpisy. Tento způsob přístupu je vázán na konkrétní počítač a v poslední době je spíše na ústupu. [1]

1.3. Soupis operací, které lze provádět pomocí Internetového bankovnictví

- zadávání jednorázových příkazů k úhradě (včetně zahraničních),
- zadávání, změnu a rušení trvalých příkazů k úhradě,
- zadávání povolení, změny či zrušení inkasa,
- hromadné platby, tj. odeslání většího množství plateb najednou,
- operace s termínovanými vklady (převod volných prostředků na termínované vklady),
- převody mezi účty v různých cizích měnách (ve výhodnějších kursech, okamžitý převod),
- podporu pro provádění opakovaných plateb, tj. přednastavení vzorů plateb, adresář příjemců plateb atd.,
- automatické zasílání informací o zůstatku na účtu, změnách zůstatku na účtu (formou SMS či e-mailem),
- zobrazování historie pohybů na účtu pro různé časové intervaly,
- získávání elektronických výpisů (v elektronické podobě, v PDF),
- komunikace s bankou pomocí zasílání různých textových zpráv přes internet,
- další služby (dobíjení kreditu mobilních telefonů, nákup a prodej podílových listů, správa úvěrových produktů atd.). [3]

1.4. Postup komunikace klienta s bankou

Mezi nástroje k zajištění bezpečnosti patří především identifikace banky, autentizace klienta (ověření identity klienta při přihlašování do Internetového bankovnictví), zabezpečení samotného přenosu dat z počítače uživatele do banky, autorizace (potvrzení)

prováděných operací. Jako jistá prevence zneužití pak může sloužit možnost nastavení různých limitů operací (např. limit bankovních transakcí) a zasílání informačních zpráv o provedených operacích (SMS, e-mailem). [3]

1.4.1. **Identifikace banky**

Identita banky je nejčastěji ověřována pomocí SSL (Secure Socket Layer) certifikátu, který slouží k ochraně odesílaných dat. Bez tohoto certifikátu by zkušený hacker mohl odposlechnout odesílaná data. Některé banky používají sofistikovanější certifikáty EV (Extended Validation), které využívají propracovanější systém ověřování totožnosti, pro uživatele patrné z adresního řádku, kde je webová adresa, nebo název banky znázorněný v zeleném rámečku. [3]

1.4.2. **Autentizace klienta**

Identifikace klienta je ověření totožnosti osoby, která vstupuje do Internetového bankovnictví. Základní a nejčastější způsob autentizace je uživatelské jméno a heslo, pro zvýšení bezpečností může být doplněn o certifikát, SMS klíč, PIN kalkulátor nebo TAN kód.[3]

1.4.3. **Zabezpečení přenosu dat**

Bezpečnost přenosu citlivých informací a klíčů transakcí je závislá na typu použitého šifrovacímu algoritmu, délce klíčů, věrohodnosti certifikátů a certifikačních autorit ale zároveň i zabezpečení klientova počítače.

1.4.4. **Autorizace prováděných operací**

Jde o dodatečné ověření a potvrzení pokynu k aktivní operaci. Pro finanční operace, jako je příkaz k úhradě, trvalý příkaz, inkaso atd., nebo změny v nastavení bankovnictví, jako jsou

změny limitů výběrů, plateb a další, je třeba transakci potvrdit zadáním autorizačního kódu. Tento kód může být opět formou certifikátu, TAN kódu nebo SMS klíče. [3]

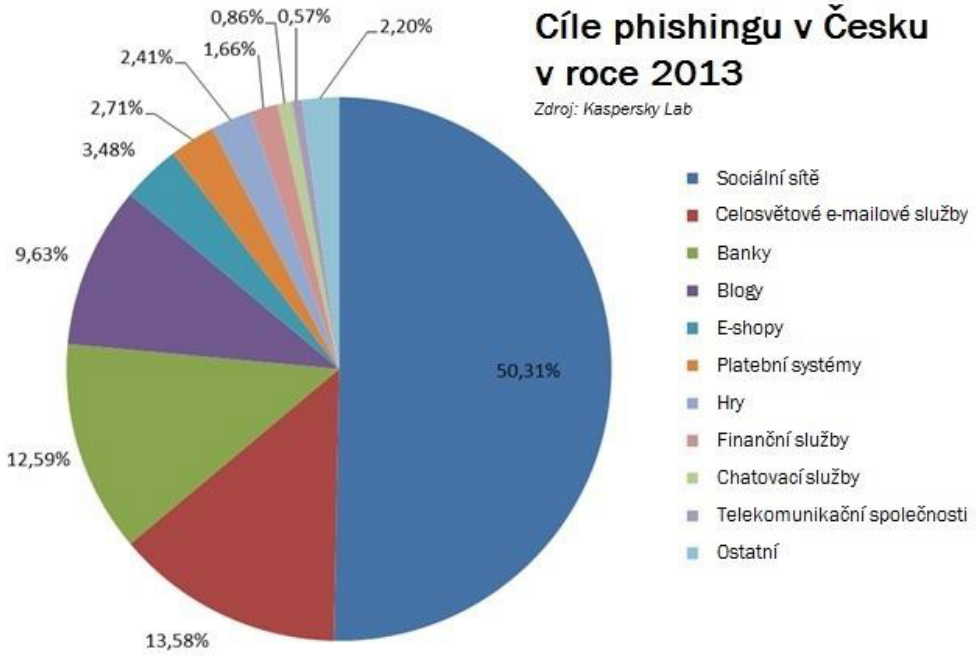
1.5. Nejčastější typy prolomení bezpečnosti

Mezi nejčastější útoky na Internetová bankovnictví patří Phishing, Heartbleed, útok na kompresi dat před šifrováním a MITM.

1.5.1. **Phishing**

„*Phishing je metoda kybernetického zločinu, při níž útočníci chtějí získat osobní informace oběti, které potom využívají k nelegální činnosti. Využívají k tomu falešné stránky imitující legitimní internetové zdroje.*“ [4] Server Feedit.cz uvádí cíle, na které se útočníci zaměřují.

Graf 3 – Cíle phishingu v Česku v roce 2013



Zdroj: [online]. [cit. 2014-04-07]. Dostupné z: http://www.feedit.cz/images//2014/04/C%C3%ADle-phishingu-v-%C4%8CR-v-roce-2013-600x432.jpg

1.5.2. **Heartbleed**

Heartbleed je útok na službu heartbeet protokolu TLS, jejíž hlavní funkcí je udržování a ověřování aktuálního spojení. Zpráva heartbeat obsahuje pole dat, které musí protistrana poslat zpět beze změn. Toto pole může být různě dlouhé, proto je definované dvoubajtovou hodnotou určující jeho délku. Chyba spočívala v tom, že OpenSSL nekontrolovalo, zda udaná délka odpovídá skutečné délce zprávy, a proto při udání větší délky byla do zprávy přidána data následující za zprávou. Tato data obsahují komunikační data včetně privátních klíčů, jmen, hesel i obsah zpráv. Tato chyba byla již na většině serverů opravena. [5], [6]

1.5.3. **Útok na kompresi dat před šifrováním**

Útok spočívá v možnosti přístupu ke komprimovaným datům, které ještě nebyly zašifrovány, protože šifrování probíhá až po kompresi dat. Útočník získá neznámá data, která mohou obsahovat libovolný obsah, tedy text zprávy, ale i citlivá data.

V praxi útok funguje nejlépe proti session cookies. Pokud útočník může sledovat síťový provoz a manipulovat prohlížečem oběti, může tak v důsledku krást cookies i unést celou relaci. V současné podobě využívá JavaScript a vyžaduje 6 žádostí extrahovat jeden byte dat. Použití JavaScript je žádoucí, ale není nutné, jednoduché <img> tagy mohou dělat svou práci stejně dobře, i když snižují výkon. [7]

1.5.4. **MITM (Man In The Middle)**

Je to útok, umožňující útočníkovi aplikovat libovolný obsah do šifrovaného toku dat. Problém je s opětovným projednáním funkcí, které umožňují jednu část šifrovaného spojení, útok se odehrává předtím, než dojde k novému projednání. Útočník může otevřít připojení k serveru SSL a odesílat data až od té chvíle, než jsou předány serveru SSL od oprávněného uživatele. Tedy webové servery budou kombinovat údaje, které obdrží od útočníka s údaji, které obdržíte po sjednání nové dohody od uživatele. Dobrou zprávou je, že i když může útočník spustit libovolný požadavek, nebude moci získat odpovídající reakci. Na druhou stranu bude klient vidět něco jiného, než to, co požaduje. [8]

2. Současné technologie

Architekturou současné technologie používání při zabezpečení internetového bankovnictví je model ISO – OSI a protokol TCP/IP.

2.1. Model ISO - OSI (6)

Tento model vznikal v druhé polovině 70. let, kde byl kladen důraz na otevřenost systémů, tak aby připojení k síti bylo možné v celosvětovém měřítku pro všechna koncová zařízení uživatelů od různých výrobců. Tento model se v roce 1984 stal normou a jeho úlohou je poskytnout základnu pro koordinované vypracování norem pro účely snadného a funkce schopného propojování otevřených systémů.

Architektura referenčního modelu OSI je sedmivrstvá, kde každá vrstva vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci s jiným systémem. Každé zařízení v síti je jednoznačně identifikovatelné pomocí MAC adresy, která má délku 48 bitů v šestnáctkové soustavě, je složena z kódu výrobce a označení fyzického rozhraní. [9]

Vrstvy modelu OSI

- Fyzická – aktivuje, udržuje a deaktivuje fyzické spoje pro přenos bitů, které jsou postaveny na úrovni mechanických a elektrických charakteristik.
- Spojová (linková) – poskytuje přístup k přenosovému prostředku, tj. jedno nebo několik dynamických spojení mezi dvěma síťovými entitami sídlícími v sousedních systémech.
- Síťová – zajišťuje síťové spojení otevřeným systémům, které spolu nemusí sousedit, přenos datových jednotek je označován jako pakety.
- Transportní – poskytuje transparentní a spolehlivý přenos s požadovanou kvalitou, zprostředkovává komunikaci mezi systémy.
- Relační – zajišťuje komunikaci mezi stanicemi, organizuje a synchronizuje dialog mezi prezentačními entitami a řídí výměnu dat mezi nimi.
- Prezentační – zajišťuje transparentní přenos zpráv mezi koncovými uživateli, nastavuje jednotnou strukturu zpráv bez ohledu na různorodost.

- Aplikační – je to rozhraní s uživatelem a procesy aplikací, poskytuje aplikačním procesům přístup ke komunikačním systémům. [10]

Model OSI je považován za úplný základ síťové technologie, ze kterého vychází současně používaný model TPC/IP. Model OSI musí při komunikaci obsahovat všechny vrstvy síťového rozhraní a zároveň umožňuje každé vrstvě komunikovat pouze s vrstvou nad nebo pod. Proto vznikl model TCP/IP, který slučuje některé vrstvy pro zjednodušení komunikace mezi vrstvami a umožňuje tak větší flexibilitu a kontrolu nad prováděnými úkony. [10]

2.2. **Protokol TCP/IP** (RFC 5000)

Protokol TCP/IP označuje celou síťovou architekturu, která tvoří jádro celého systému. Od počátku vzniku protokolu TPC/IP byl kladen důraz na budování otevřeného systému pro propojování jednotlivých sítí, který umožňuje oprostit se od závislosti na síťové infrastruktuře a vnímat sítě (včetně internetu) propojené směrovači jako jednu velkou síť. Pro uživatele se internet jeví jako virtuální síť, k níž se počítače (hosts) připojují. Ve skutečnosti je internet soubor vzájemně propojených a spolupracujících fyzických sítí, přičemž každý komunikační systém schopný přenášet datové pakety se bere jako síť. [10]

Tabulka 1 – Srovnání vrstev protokolu TCP/IP a modelu ISO/OSI

TCP/IP	Model ISO/OSI
Aplikační vrstva	Aplikační vrstva
	Prezentační vrstva
	Relační vrstva
Transportní vrstva	Transportní vrstva
Síťová (IP) vrstva	Síťová vrstva
Vrstva síťového rozhraní	Linková vrstva
	Fyzická vrstva

Zdroj: [online]. [cit. 2014-04-09]. Dostupné z:http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A1_architektura#mediaviewer/Soubor:Porovn%C3%A1n%C3%AD_TCPIP_a_modelu_ISOOSI.jpg

Vrstvy protokolu TCP/IP:

2.2.1. Vrstva síťového rozhraní

Je nejnižší vrstva architektury TCP/IP umožňující přístup k fyzickému přenosovému médiu. Úkolem vrstvy je zapouzdřit datagramy IP do rámců odpovídajících formátů a délek pro přenos daným rozhraním a zároveň slouží pro mapování síťových adres (IP) na adresy fyzické (většinou MAC). V současné době může protokol IP využívat všechny typy přenosových prostředí: lokálních sítí LAN (Ethernet, Token Ring, FDDI) i rozlehlých sítí WAN (ATM, X.25, a další). [10], [11]

2.2.1.1. Lokální sítě LAN

Lokální síť LAN je komunikační síť propojující koncové uzly jako osobní, pracovní stanice, servery, terminály umožňující jejich vzájemnou spolupráci. Jsou omezeny nejčastěji do několika kilometrů, většinou ale působí v rámci jedné budovy nebo patra. Pro připojení k lokální síti je zapotřebí karta síťového rozhraní, která slouží k vysílání a přijímání rámců LAN. Pracují v režimu bez spojení, odesílatel tedy nepotřebuje navazovat spojení s příjemcem, není s ním v neustálém kontaktu a nezjišťuje, zda je příjemce dostupný nebo zda vůbec existuje. [10]

2.2.1.2. Rozlehlé sítě WAN

Rozlehlá síť WAN umožňuje komunikaci mezi koncovými uzly, stanicemi, lokálními nebo metropolitními sítěmi na velkou vzdálenost. Pracují v režimu se spojením a mnohonásobným přístupem tak, že data vysílaná jedním uzlem se v běžném přenosovém režimu dostanou pouze k adresátovi. Sítě WAN zpravidla poskytují přenosové prostředí, nikoli uživatelské aplikace přímo v síti.

Rozhraní přístupu k síti je ohraničení dvěma zařízeními DTE a DCE. Koncové datové zařízení DTE se skládá z datového zdroje vysílajícího data a datového spotřebiče, zachycujícího data, které spravuje řídící jednotka (řadič). Ukončující datové zařízení DCE

transformuje digitální signál na signál schopný přenos po přenosových kanálech (např. modem transformuje digitální signál na analogový). [10]

2.2.2. **Síťová vrstva (mezisíťová vrstva, vrstva internetu)**

Mezisíťová vrstva odpovídá svými funkcemi a službami vrstvě síťové referenčního modelu ISO - OSI. Mezi její funkce patří především směrování (routing) a přepojování/předávání (forwarding) datagramů přes komunikační podsíť, což zajišťuje jednotné schéma IP adresace a definice formátu IP diagramu. Zároveň musí mezisíťová vrstva jednoznačně definovat rozhraní se sousední transportní vrstvou a vrstvou síťového rozhraní. Mezi základní protokoly této vrstvy patří protokol IPv4 a protokol IPv6. [10], [11]

Protokol IP verze 4 (IPv4) (RFC 791)

Protokol IPv4 vysílá datagramy na základě síťových adres obsažených v jejich záhlaví a poskytuje síťovou službu bez spojení. Protokol IP tedy nenavazuje spojení pro přenos diagramů, ani neudržuje žádné informace o datagramech, které předává dál. Protokol IP nemá v sobě zabudovaný žádný mechanizmus pro detekci a korekci chyb v přenášených datech, proto se spoléhá na protokoly vyšších vrstev, kontroluje pouze správnost záhlaví IP datagramu. Nespolehlivost protokolu vede ke ztrátě, duplikaci, přijetí datagramů v jiném pořadí nebo se zpožděním. Vrstva dále provádí fragmentaci a opětovné sestavování datagramů do a z rámců specifikovaných protokolem nižší vrstvy. [10]

Protokol IP verze 6 (IPv6) (RFC 2460)

Nová verze protokolu IPv6 byla vypracována již v roce 1995 z důvodu nedostatečné adresové a směrovací podpory předchozí verze IPv4, která nabízí pouhé 4,3 miliardy jedinečných adres. Nárůst požadavků na nové adresy souvisí nejen s rozšiřováním sítí a neustálým vývojem nových inteligentních bezdrátových technologií, ale také v důsledku nesystematického přidělovaní adres a směrování poskytovateli internetového připojení. Protokol IPv6 tyto problémy řeší, a to tímto způsobem:

- Výrazně rozšířený adresní prostor poskytující 10^{38} jedinečných adres.
- Zjednodušení formátu záhlaví diagramu.
- Povinná podpora pro IPSec.
- Rozšířená podpora pro Mobilní IP.

Důvodem, proč ještě plně nevyužíváme IPv6, je složitost přechodu ze stále se rozšiřujících sítí IPv4. Složitost přechodu spočívá v tom, že by byla zapotřebí kompletní readresace z IPv4 na IPv6 a nákladné změny zařízení a software. Z tohoto důvodu se objevila dočasná řešení spočívající v:

- Překladu síťových adres NAT umožňující omezení spotřeby globálně rozpoznatelných adres v koncových sítích.
- Adresaci podsítí s proměnnou délkou masky.
- Směrování bez ohledu na třídy IPv4. [10]

2.2.3. **Transportní vrstva**

Je vrstva v podstatě odpovídající transportní vrstvě referenčního modelu ISO - OSI, která se stará o koncový přenos datových jednotek mezi odesílatelem a příjemcem. Služba, kterou vrstva nabízí, může být buď spolehlivá (TCP), která garantuje doručení všech dat v pořadí jejich odeslání, nebo nespolehlivá (UDP), která negarantující ztráty při přenosu negarantuje. [10], [11]

2.2.3.1. **Protokol TCP** (RFC 793)

Je transportní protokol se spojením, poskytuje logické spojení mezi koncovými aplikacemi, které využívají ke své práci aplikační protokoly vyžadující spolehlivou transportní službu jako je např. FTP, TELNET. Protokol TCP je bitově orientovaný a přijímá informace od vyšší vrstvy jako souvislý tok bitů, který musí rozdělit do transportních segmentů délky odpovídající velikosti datagramu IP, která předá síťové vrstvě. Protokol TCP pracuje na principu spojení, které je definováno dvěma koncovými body (stanice, port) a proto je možné sdílet jeden port pro více spojení na jedné stanici. [11]

Vlastnosti protokolu TCP:

- Spolehlivost transportní služby – doručí adresátovi všechna přenášená data, bez ztráty nebo zkreslení dat.
- Plně duplexní spojení – současně obousměrný přenos dat.
- Efektivní využití přenosových kanálů – využívá vyrovnávací paměť a začne vysílat, až pokud nashromáždí dostatek dat, nebo vyprší časový limit.
- Ochrana proti zahlcení.
- Podporuje libovolně dlouhé bloky dat.

2.2.3.2. **Protokol UDP** (RFC 768)

Je velmi jednoduchý transportní protokol, který poskytuje nespolehlivou transportní službu pro aplikace nevyžadující zabezpečení v takovém rozsahu, jaké využívá protokol TCP. U tohoto protokolu tedy doručení dat bez ztráty, zkreslení, duplicity nebo doručení v pořadí musí zajistit aplikační program. Protokol UDP pouze podporuje komunikaci mezi koncovými procesy, nikoli mezi koncovými uzly a podporuje vysílání na všeobecnou IP adresu a skupinové adresy. Transportní protokol UDP se využívá při malém objemu dat např.: dotaz – odpověď, potvrzení o přijetí dotazu. Pokud odpověď dlouho nepřichází, tak aplikace vyšle dotaz nový. UDP je vhodnější pro provoz v reálném čase, ale kvůli své jednoduchosti ve specifikaci přenosu je třeba další doplňující protokol RTP. [10], [11]

Protokol RTP

Je přenosový protokol, zajišťující podporu pro koncové multimediální přenosy v reálném čase, pracující nejčastěji na protokolu UDP. Protokol RTP však nezaručuje doručení dat ani správné pořadí paketů, ale do záhlaví přidá pořadová čísla a typ paketů, podle kterého aplikace dokáže rozeznat chybějící pakety. Protokol byl navržen pro jednosměrný i obousměrný přenos a využívá se nejčastěji pro videokonference. [10]

2.2.4. **Aplikační vrstva**

Je nejvyšší vrstvou síťové architektury a obsahuje všechny protokoly poskytující uživatelům konkrétní aplikace. Aplikačními protokoly jsou protokoly pro vzdálený přístup (TELNET, SSH), přenos souborů (FTP, SCP, SFTP), přístup k serveru e-mailových zpráv (SMTP,POP,IMAP), sdílení vzdálených souborů (NFS), mapování adres a jmen (DNS), synchronizaci času (NTP) a bezpečnostní aplikace (KERBEROS, RADIUS).

- TELNET - Protokol pro vzdálený přístup (RFC 854)

Je protokol virtuálního terminálu, umožňující přihlášení ke vzdálenému počítači tak, že jeho pracovní prostředí vypadá, jako by byl připojen přímo. Uživatel využívá svůj lokální hardware (monitor, myš, klávesnici), vzdálený software a počítač s možností přístupu k datům a tiskárnám. Pro vytvoření relace mezi vzdálenými počítači je z důvodu zabezpečení zapotřebí identifikace, která se ve většině případů skládá z uživatelského jména a hesla v nešifrované formě. „TELNET pracuje na principu klient-server tak, že klient zřídí spojení se serverem a posílá mu jednotlivé znaky tak, jak jsou psány na klávesnici, server je pak zpracovává, jako by byly psány na lokálním terminálu a vzniklé výstupní znaky opět pošle klientovi, který je pak lokálně zobrazí“ [10]

- SSH - Protokol pro vzdálený přístup (RFC 4253)

Je zabezpečený komunikační protokol pro vzdálený přístup, který vznikl v reakci na špatně zabezpečený protokol TELNET. Protokol SSH umožňuje bezpečně vzdáleně spravovat počítač a bezpečně kopírovat data. V širším využití umožňuje administraci serverů nebo vytvoření virtuální privátní sítě a její správu. Nejčastěji se SSH používá mezi Unixovými systémy. „*Ve Windows si můžeme SSH server zřídit pomocí aplikací třetích stran: některé jsou zdarma a s otevřenými kódy, jiné jsou placené, přičemž pro domácí a nekomerční použití bývají zdarma.*“ [12]

- FTP – Vzdálený přenos souborů (RFC 959)

Umožňuje jednoduchým způsobem přenos souborů mezi uzly připojenými k internetu, např.: k přesunu dokumentů na server, odkud k dokumentům mají přístup i ostatní uživatelé, ke stahování volně šiřitelných programů do svého PC a další. Klient buď musí projít přihlašovacím procesem (jméno, heslo) nešifrovaným spojením, nebo jsou data volně dostupná bez znalosti hesla. FTP využívá spolehlivou transportní službu se spojením typu klient-server poskytující dvě spojení, řídící a datové. Po řídícím spojení jsou přenášeny příkazy a odpovědi, určuje čísla portů pro datové spojení a existuje po celou dobu relace. Po datovém spojení jsou přenášena výhradně data. [10], [11]

- SCP a SFTP - Vzdálený přenos souborů (RFC 4253)

SCP je jednoduchý protokol, který dovoluje kopírovat soubory ze serveru a na server pomocí zabezpečeného SSH protokolu. Dnes všechny SSH servery využívají novější protokol SFTP. „*Výhody jsou zcela zřejmé: kompletně šifrovaný přenos, jeden standardní port, velké množství klientů, možnost přihlašování pomocí klíčů a další.*“ [13]

- SMTP, POP, IMAP – Elektronická pošta (RFC 5321)

Jednoduchý protokol pro transfer elektronické pošty mezi stanicemi, využívající protokoly POP nebo IMAP pro přístup ke zprávám a protokol SMTP pracující jako střadač, kde jsou uloženy odeslané zprávy, dokud si je příjemce nevyzvedne. SMTP dále zajišťuje předávání poštovních zpráv na principu klient-server, kde klient zprávu předává a server zprávu přebírá. [10]

- NFS – Sdílení vzdálených souborů (RFC 3530)

Jedná se o distribuovaný systém souborů na síti, který umožňuje transparentní sdílení vzdálených souborů na síti, jako by byly lokální. NFS nejčastěji využívá protokol UDP a pracuje v režimu klient-server. Byl navržen pro lokální sítě, u kterých se očekává vysoká spolehlivost, rychlá odezva a synchronizace v čase. [10]

- DNS – Mapování jmen a adres (RFC 1035)

Stará se o mapování (překlad) doménových jmen na platné 32bitové adresy IPv4, které využívají téměř veškeré aplikace jako FTP, TELNET, SMTP atd. Mapování je automatické, jak z pohledu uživatele, tak i běžících programů. Je založené na komunikaci koncového počítače se serverem DNS, musí znát adresu serveru DNS, nebo mít možnost adresu získat dynamicky (DHCP). V čele hierarchie je 13 kořenových serverů, na které navazují primární servery a sekundární servery. „*Kořenové servery obsahují IP adresy všech autorizovaných registrů vrcholových domén, tedy jak schválených gTLD (generic Top Level Domain), tak všech téměř 250 registrů ccTLD (country-code Top Level Domain).*“ [14] Primární servery ukládají soubor o zóně, který spravují. Sekundární servery pouze přenáší informace o zóně z jiného serveru.

- NTP – Síťový protokol času (RFC 1035)

Slouží k synchronizaci hodin v rámci sítě a mezi uzly, což je důležité pro práci v reálném čase a pro bezpečnostní systémy. Umožňuje koncovým uzlům přesný čas podle atomových hodin. [11]

- KERBEROS, RADIUS – bezpečnostní aplikace v kapitole 3.7.1 a 3.7.2.

2.3. Způsoby zabezpečení při přihlašování k Internetovému bankovnictví

K přihlašování do Internetového bankovnictví se vždy využívá uživatelské jméno a heslo, které může být rozšířeno o SMS kód, certifikát uložený v PC nebo na čipové kartě, PIN kalkulátor, TAN kódy nebo biometrické zařízení.

2.3.1. **Uživatelské jméno a heslo**

Uživatelské jméno a heslo je nejjednodušším, ale zároveň nejméně bezpečným způsobem zabezpečení internetového bankovnictví. Některé banky umožňují v tomto případě pouze pasivní operace (tj. zjistit stav a pohyby na účtu, nikoli však zadávat platební příkazy). Zabezpečení je náchylné nejen na vyzrazení hesla a uživatelského jména, ale také na „odposlech" klávesnice. Proto bývá tento způsob přihlašování rozšířen o další bezpečnostní prvky. [15]

2.3.2. **SMS Kód**

Kód zasílaný prostřednictvím SMS zpráv je nejoblíbenějším způsobem zabezpečení. Využívají se dvě možnosti - klasická SMS zpráva, která je méně bezpečná, a šifrovaná SMS s využitím tzv. SIM Toolkitu. V tomto případě je třeba dbát na bezpečnost mobilního telefonu. Dále se využívá k potvrzování transakcí. [15]

2.3.3. **Certifikát**

Podpisový certifikát neboli elektronický podpis uložený v souboru slouží k ověření identity klienta. Jeho nevýhodou je možnost zkopírování certifikátu a jeho následného zneužití. Certifikát by měl být uložen na přenosném médiu, které uživatel připojuje k počítači při využívání internetového bankovnictví. Zásadní chybou je uložení certifikátu na pevném disku v počítači, nebo dokonce na internetu. Bezpečnější jsou certifikáty na čipové kartě či iKey tokenu. Pro zvýšení bezpečnosti rovněž lze podpisový certifikát ochránit heslem, které bude při použití vyžadováno. [15]

2.3.4. **Certifikát na čipové kartě**

Elektronický podpis je generován pomocí certifikátu uloženého na čipové kartě, který nelze zkopírovat. Případný útočník by musel získat kartu i hesla, která ji chrání. [15]

2.3.5. **PIN kalkulátor**

PIN kalkulátor je generátor hesel pro vstup a pro ověření transakcí. Klient pro ověření pokynu musí zadat atributy transakce i do kalkulátoru, a na jejich základě je mu vygenerován PIN. Jedná se o jeden z nejbezpečnějších způsobů ověření. Novinkou je kombinace generátoru jednorázových hesel s čipovou kartou, kterou přinesla BAWAG Bank. [15]

2.3.6. **TAN kód**

TAN kódy jsou jednorázové kódy zasílané zpravidla poštou, které slouží k ověření klienta i potvrzení transakce. Klientovi je vydána vždy sada hesel (zpravidla 50 až 100), po jejichž spotřebování obdrží nová. Tento systém je poměrně bezpečný, nebezpečím je ale případná ztráta kódů. [15] U nás TAN kódy využívá banka Oberbank. Pro přihlášení se použije uživatelské jméno a heslo, jestliže chcete vykonat bankovní operaci, zadáte jednorázový kód TAN, který se použitím zneplatní. [16]

2.4. Biometrie

Dnes se zcela běžně představa biometrie spojuje s identifikací lidí pomocí unikátních charakteristických rysů. Odborně tato disciplína zkoumá biologické rysy, které jsou pro každého člověka jedinečné a neměnné. V elektronickém bankovnictví se jedná především o "vlastnoruční biometrický podpis". Jedná se o podpis klienta, který je prováděn hrotem na elektronickém tabletu (signpady). Takový podpis jak vizuální podobu, tak vlastní elektronický obraz pro další porovnávání (včetně biometrických charakteristik). [17]

Signpady zaznamenávají kromě grafické podoby podpisu i další parametry, například tlak na podložku, rychlost, směr tahu, akceleraci i úhel podpisu klienta a zvyšují tak pravděpodobnost shody s podpisovým vzorem. [18]

Elektronický podpis vymezuje Zákon č. 227/2000 Sb., o elektronickém podpisu, ve kterém jsou stanoveny následující požadavky:

- Je jednoznačně spojen s podepisující osobou.
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
- Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. [19]

Signpady využívá např. GE Money Bank, která svým klientům umožňuje podepisovat dokumenty elektronicky a tím nahrazuje papírové dokumenty. Zákazníci tak více komunikují s bankou elektronicky, ale pokud se do banky musí dostavit osobně, tak neodcházejí s deskami plnými papírů, ale všechny dokumenty jsou přístupné v elektronické podobě a to v plném znění včetně dodatků. Do konce roku 2014 GE Money Bank zprovozní biometrická zařízení na všech pobočkách v České republice. [18]

3. Technologie zabezpečení

Cílem bezpečnostních protokolů a služeb je především zamezit množící se bezpečnostní rizika, která mohou mít v sítích různé závažné důsledky, na jejichž základě dochází ke ztrátě a možnému zneužití citlivých dat nebo odcizení identity. Za bezpečnostní technologii se považuje:

- Bezpečnostní politika
- Šifrování
- Digitální podpis
- Digitální certifikát
- SSL a TSL
- Virtuální privátní sítě VPN
- Bezpečnostní aplikace aplikační vrstvy
- Firewall

3.1. Bezpečnostní politika

Bezpečnostní politika je postavena na principu rozpoznání autorizovaného a neautorizovaného chování. Je založena na pravidlech a identitě, která jsou jednoznačně stanovena, za použití různých mechanizmů slouží k prevenci, detekci a nápravě. Do bezpečnostní politiky patří:

- Důvěrnost dat – Ochrana dat před neautorizovaným únikem informací je zajištěna pomocí kódování a šifrováním, která v případě nepoužití správného šifrovacího mechanizmu nelze přečíst.
- Autentizace uživatele – Ověření totožnosti, zda uživatel je opravdu ten, za koho se vydává, může být zajištěno pomocí hesla, digitálního podpisu, biometrického zařízení atd.
- Integrita dat – Ochrana proti neautorizované změně dat, jejich zničení nebo duplicity posílaných dat. Odeslaná data musí být identická s přijatými daty.
- Řízení přístupu – Přidělení přístupových práv k určitým oblastem na základě identifikace uživatele.

- Nepopiratelnost zprávy – Ochrana proti odmítnutí přijetí nebo vyslání zprávy pomocí důkazu o doručení nebo původu zprávy. [10], [11]

3.2. Šifrování

Jedním z hlavních úkolů zajištění bezpečnosti komunikace je utajení citlivých přenášených dat související s nárůstem jich množství. Šifrování představuje účinnou formu, jak zamezit neoprávněným osobám přístup k soukromým datům, přihlašovacím údajům, elektronickému bankovnictví, přenášeným souborům atd. Používají se dvě základní metody šifrování, symetrické šifrování a asymetrické šifrování.

3.2.1. **Symetrické šifrování**

Symetrické šifrování je šifrování jediným klíčem, který sdílejí obě strany komunikace a užívá se jak pro šifrování, tak i k dešifrování. Klíče jsou většinou krátké z důvodu rychlosti a jednoduchosti algoritmických výpočtů. Nevýhodou tohoto šifrování je jeho samotné zabezpečení při přenosu sítí, neboť je klíč distribuován všem uživatelům, kteří ho potřebují. Při tomto šifrování se používají dva základní typy klíčů a to DES a AES. [20]

DES klíč

Je klíč o délce 56bitů a nabízí přibližně 7,2 x 10^{16} kombinací možných klíčů. Používá se většinou pro ochranu tajemství druhé největší priority. Zesílení šifrování lze dosáhnou trojitým použitím DES tedy 3DES, který je ale třikrát pomalejší. [10]

AES klíč (RFC 3268)

Je založen na Rijndaelovu algoritmu, který umožňuje použití klíčů o délce až 256 bitů, kde vytváří až 1,1 x 10^{77} kombinací klíčů. AES se využívá v rámci zabezpečení přenosu na úrovni transportní vrstvy protokolu TCP. [10]

3.2.2. **Asymetrické šifrování**

Při asymetrickém šifrování se pro šifrování a dešifrování používají dva klíče, a to soukromý, který vždy zůstává tajemstvím, a veřejný, který je dostupný každému. Pokud je zpráva zašifrována veřejným klíčem, lze jí dešifrovat pouze odpovídajícím soukromým klíčem, který nelze odvodit z komunikace, protože není přenášen po síti, ale je uložen v příjemcově počítači. V tomto případě asymetrické šifrování slouží k ochraně přenášených dat, ale ne k autentizaci odesílatele zprávy. Pokud k šifrování odesílatel použije soukromý klíč, může zprávu dešifrovat kdokoliv, ale odesílatel je jednoznačně autentizován a nemůže popřít, že je autorem zprávy. Nevýhodou asymetrického šifrování je složitost použitého algoritmu, a proto se často využívá kombinace asymetrického šifrování pro zašifrování a symetrického šifrování pro bezpečnou distribuci symetrických klíčů. Asymetrické šifrování využívají dvě základní metody šifrování D-H a RSA. [20]

D-H (Diffie-Hellman) metoda

Nepoužívá se pro šifrování dat, ale pro bezpečnou distribuci klíčů mezi dvěma stanicemi, tento klíč pak šifruje datový šifrovací klíč. Nevýhodou D-H je neautentizace mezi zařízeními, proto je potencionálně napadnutelný útoky typu man-in-the-middle.

Princip:

1. Server si vygeneruje soukromý klíč a z něj odvozený veřejný klíč pošle klientovi.
2. Klient si vygeneruje svůj soukromý klíč a veřejný pošle na server.
3. Server spojí svůj soukromý klíč s klientovým veřejným, klient svůj soukromý se serverovým veřejným.
4. Díky vlastnostem algoritmu vyjde oběma to samé, což ustanoví heslo používané pro šifrování další komunikace. [20]

RSA metoda

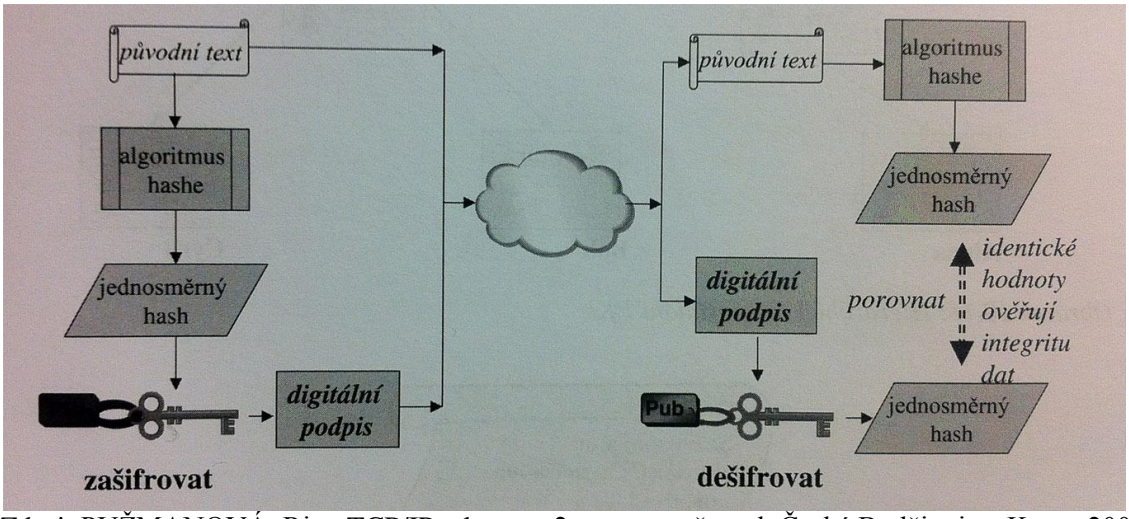
Je první algoritmus, který je vhodný jak pro šifrování, tak pro elektronický podpis. Algoritmus je považován za bezpečný při požití délky klíče 1024-2048 bitů. „*Bezpečnost RSA je postavena na předpokladu, že rozložit číslo na součin prvočísel (faktorizace) je*

velmi obtížná úloha.“ [21] Algoritmus lze použít jak pro šifrování, tak autentizaci v el. poště, virtuálních privátních sítích, webového zabezpečení pomocí SSL atd. [21]

3.3. Digitální podpis

Slouží k ověření, zda zpráva pochází od odesílatele a potvrzuje, že obsah zprávy nebyl při přenosu pozměněn. Na otevřený text aplikuje odesílatel hashovací funkci a obdrží „otisk“ otevřeného textu, který je pevné délky několika bajtů. Otisk pak zašifruje odesílatel svým soukromým klíčem algoritmu asymetrického šifrování. Svazuje tedy zprávu se soukromým klíčem odesílatele, který zle dešifrovat pouze pomocí veřejného klíče. Ten získá původní hashovaní řetězec a obě hodnoty hashe porovná, v případě, že vše souhlasí, může potvrdit totožnost odesílatele. [22]

Obrázek 1 – Digitální podpis



Zdroj: PUŽMANOVÁ, Rita. TCP/IP v kostce. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, s. 513. ISBN 978-80-7232-388-3.

3.4. Digitální certifikát

Je soubor informací jednoznačně identifikující uživatele nebo zařízení. Obsahuje jméno, sériové číslo, společnost, oddělení, IP adresu, životnost certifikátu a také kopii veřejného

klíče držitele certifikátu. Kvalita certifikátu je dána několika faktory: důvěryhodností certifikační autority, která certifikát vydala, typem použitých šifrovacích algoritmů a transparentním ověřením softwaru a uživatele ověřujícího certifikát.

3.5. Protokoly SSL a TLS

Protokoly SSL a TLS slouží k zabezpečení na transportní a aplikační vrstvě pro síťovou komunikaci. Protokoly TLS a SSL jsou protokoly poskytující šifrování dat a autentizaci mezi uživatelem a serverem v případech, kde jsou data přenášena po nezabezpečené síti. Jsou to ověřené metody pro zabezpečení citlivých dat komunikace přes webový server a jejich hlavní priority jsou důvěrnost, integrita a dostupnost. [10]

3.5.1. **Protokol SSL** (RFC 4346)

Protokol SSL zajišťuje autentizaci uživatele, integritu dat a šifrování aplikačních dat při přenosu přes veřejnou IP. Využívá protokolu TCP, k autentizaci využívá jména a hesla (RADIUS), jména a token (RSA SID), nebo digitální certifikát X.509. Šifrování je zajištěno pomocí kombinace veřejného a soukromého klíče. Protokoly SSL používají spojení, logický spoj, poskytující služby mezi klientem a serverem a relace tvořené pomocí protokolu handshake a definující sadu bezpečnostních opatření. Nejčastěji se SSL využívá k zabezpečení protokolu HTTP označovaného HTTPS.

Princip:

Protokol SSL je konstruován ve dvou úrovních, a to vrstvy záznamů a protokolu CCS. „*Vrstva záznamů je zodpovědná za fragmentaci a někdy kompresi aplikačních dat, šifrování a autentizaci dat prostřednictvím algoritmů symetrických klíčů. Klíče se stanoví v průběhu počátečního dojednávání (protokol handshake), které používá algoritmy asymetrického šifrování na vytvoření hlavního soukromého klíče mezi klientem a serverem.*“ [10] Nejčastěji se používá jednosměrná autentizace ze strany serveru a klient se

dále autentizuje heslem.„ Protokol CCS se používá na signalizaci úspěšného navázání spojení protokolem handshake, tedy signalizace pro zahájení autentizace a šifrování toku dat. [11]

3.5.2. **Protokol TLS** (RFC 5246)

Protokol TLS vychází z protokolu SSL verze 3 a je postaven na stejném principu, ale obsahuje řadu vylepšení. Základem TSL jsou dva protokoly. TSL Record Protokol využívající symetrické šifrování, které může být zajištěno pomocí Hashovací funkce a Handshake protokol, pomocí kterého dojde k dohodě o délce šifrovacího algoritmu a volbě klíčů. TLS zahrnuje řadu bezpečnostních opatření mezi která patří:

- Ověření digitálního podpisu na serverovém certifikátu.
- Ověření doby životnosti certifikátu.
- Ověření certifikační autority.
- Ochrana před několika typy útoků včetně MITM.

Spolehlivost spojení zaručuje kontrola integrity s použitím klíče MAC a bezpečné hashovací funkce např. SHA-1. [10], [11]

3.6. VPN – Virtuální privátní sítě

„VPN je neveřejná páteřní síť využívající veřejnou komunikační infrastrukturu, kterou může být Internet, veřejná síť na bázi protokolu IP, veřejná ATM nebo Frame Relay.“ [10] VPN si ale zachovává charakter privátní sítě. Na hranici mezi veřejnou a privátní sítí stojí brána VPN, umožňující přístup pouze autorizovaným uživatelům. Sítě VPN jsou specifické efektivním využitím veřejných sítí a komunikačních služeb. Při VPN se používá služba IPSec. [10]

Služba IPSec

Je bezpečnostní architektura poskytující silné zabezpečení na bázi šifrováni pro IPv4 a IPv6. Podporuje autentizaci, integritu a důvěryhodnost na úrovni datagramů, obsahuje bezpečnostní protokoly AH a ESP a mechanizmy pro správu šifrovacích klíčů ISAKMP a IKE. [10]

3.7. Bezpečnostní aplikace Aplikační vrstvy

Mezi bezpečnostní aplikace pracující na aplikační vrstvě protokolu TCP/IP patří především protokol KERBEROS a služba RADIUS.

3.7.1. **Protokol KERBEROS** (RFC 4120)

Je autentizační protokol založený na principu důvěryhodné třetí strany využívající asymetrické šifrování. Pro ověření identity v nechráněné síti používá důvěryhodný centralizovaný autentizační server, který je zodpovědný za udržování databáze entit a jejich klíčů. Autentizace klienta neprobíhá vůči serveru, ale k autentizačnímu serveru TGS, který vydá klientovi lístek TGT s časovou platností. Od této doby autentizace za klienta provádí server TGS, kterému se klient prokazuje automaticky, bez opětovného zadání přihlašovacích údajů, pomocí lístku TGT. Kerberos má přísné požadavky na synchronizaci času klientů a serverů, proto při rozdílných časech autentizace neproběhne.

3.7.2. **Služba RADIUS** (RFC 2865)

Je služba pro autentizaci vzdálených uživatelů zahrnující všechny tři složky architektury AAA. Pracuje na principu klient-server, obsahuje protokol, server pro autentizaci (RADIUS server) a server pro klienty (NAS) a využívá transportního protokolu UDP. Obvykle se používá pro server pro telefonické připojení, server VPN nebo bod bezdrátového přístupu. [10]

3.8. Firewall

Firewall zajišťuje ochranu před útoky z vnějšku a neovlivňuje provoz v síti. Firewall neobsahuje žádná data ani prostředky pro neoprávněný přístup do sítě. Předpokladem je průchod veškeré komunikace právě přes firewall. „*Dnešní firewally brání různému "obcházení" a směruje veškerý provoz do místa, kde tento může být kontrolován. Zde pak je druhá hlavní část, která má naopak "povolovací" charakter - rozhoduje o tom, jaký druh provozu bude akceptován a propuštěn do chráněné sítě, a jaký provoz naopak bude odmítnut*.“ [23]. Firewally dělíme na paketové, pracující na síťové vrstvě, stavové, operující na transportní vrstvě a aplikační na aplikační vrstvě protokolu TCP/IP. Prvky firewallu tvoří servery a směrovače a poskytují následující funkce:

- Filtrace paketů (Paketový filtr)

  První a nejdůležitější metoda firewallu je filtrace paketů probíhající na úrovni síťové vrstvy na základě IP adres odesílatele a příjemce při prohlížení záhlaví ve spolupráci s překladem IP adres. Na směrovači je nastaven přístupový seznam, který jednoznačně dělí datagramy na povolené a zakázané. Blokace paketů probíhá nejen směrem dovnitř, ale i směrem ven z důvodu zamezení útokům zevnitř. [10]

- Aplikační firewall

  Kontroluje komunikaci na úrovni aplikační vrstvy. „*Umožňuje snadno identifikovat, klasifikovat a vynucovat zásady na základě aplikací nebo obsahu specifického pro určité aplikace. Aplikační firewall nabízí správcům seznam předdefinovaných a vlastních akcí, které kromě pravidelných aktualizací signatur umožňují vynucovat správu přenosového pásma a posílat vlastní zprávy a upozornění koncovým uživatelům.*“ [24]

- Proxy server

  Je prostředník, zástupný server, který stojí mezi klientem a skutečným (cílovým) serverem v síti. Zástupný server udržuje informace o spojení, číslech paketů a

zpracovává klientovi požadavky, které přehodnocuje a rozhoduje, zda klientovi umožní přístup či ne. [10]

- Řízení přístupu

  Ověřuje totožnost uživatele na základě hesla a jeho autorizaci pro požadované služby.

- Šifrování zpráv

  Zabezpečuje přenos informací – jmen, hesel, dat apod.

4. SWOT analýza

V praktické části této práce jsem se zaměřil na hodnocení Internetového bankovnictví vybraných bank převážně na základě zabezpečení, ale i uživatelského rozhraní a funkcí, které online bankovnictví poskytuje. Pro zhodnocení Internetového bankovnictví v této práci byly vybrány banky Air Bank a.s., Česká spořitelna a.s., Komerční banka a.s. a Československá obchodní banka a.s.. V první části jsou uvedeny základní informace o zkoumaných bankách a jejich produktech. Ve druhé části jsou sepsány produkty, které banky umožňují na svém Internetovém bankovnictví a pro porovnání jsou vyobrazeny přihlašovací rozhraní a grafická prostředí jednotlivých bank s nejběžnějšími operacemi. Ve třetí části práce jsou popsána zabezpečení jednotlivých bank, které banky uvádějí na svých webových stránkách. Ve čtvrté části jsou banky testovány pomocí online SSL Server Testu, který ověřil jejich zabezpečení. V předposlední části jsou výsledky testů setříděny do tabulky pro výsledné vyhodnocení. Na závěr praktické části práce je uveden vlastní průzkum pomocí dotazníkové metody, který se týká spokojenosti s Internetovým bankovnictvím a jeho zabezpečením.

4.1. Základní informace o vybraných bankách

4.1.1. **Air Bank a.s.**

Je jedním z bankovních nováčků, pohybující se v českém bankovním sektoru od listopadu 2011. Banka se představuje jako moderní banka 21. století pro všechny, kteří využívají běžné bankovnictví a chtějí mít banku, která se k nim bude chovat otevřeně, pravdivě a bude je považovat za zákazníky, ne za čísla. Air Bank a.s. konkuruje ostatním bankám v těchto oblastech:

- Ceník služeb se vejde na jednu stránku. Zpoplatněný úkon, má stejnou cenu, ať už ho učiníte přes Internetové bankovnictví, telefon nebo na pobočce. Banka v souvislosti s ceníkem také slibuje, že v něm nikdy nenaleznete žádný absurdní poplatek. [25]

- TOP 3 garance zaručuje, že osobní účet bude úročený nejhůře jako třetí nejlepší spořicí účet na trhu.
- Možnost výběru hotovosti na terminálech Sazky. Těch je v současné době po celé republice přes 4300. Vybrat však jednorázově půjde maximálně tři tisíce korun.
- Delší otevírací doba, od pondělí do soboty do 19 hodiny.
- Možnost vyzkoušet banku po dobu tří měsíců zdarma. [26]

Banka nabízí tyto produkty: [26]

- Běžné účty
- Spořicí účty
- Spotřebitelské úvěry

4.1.2. **Česká spořitelna a.s. (ČS)**

Je bankou, jejíž historie sahá až do roku 1825, od roku 2000 je členem rakouské Erste bank a v dnešní době se stará o více než 5,2 milionů klientů, kterým vydala více než 3,2 milionů karet. Internetové bankovnictví využívá více než 1,5 milionů klientů. ČS disponuje sítí 651 poboček a provozuje více než 1509 bankomatů. Banka má silné postavení v českém bankovním sektoru. V soutěži Fincentrum získala Česká spořitelna a.s. již po desáté ocenění Nejdůvěryhodnější Banka roku. Banka je hodnocena jako nejlepší banka v České republice i v zahraničních soutěžích, např. dle amerického časopisu Global Finance a anglického magazínu Euromoney. [27]

Banka nabízí tyto produkty: [28]

- Osobní účty
- Spořicí účty
- Spotřebitelské úvěry
- Termínované vklady
- Hypotéky
- Jistotní účty
- Vkladní knížky
- Stavební spoření

4.1.3. **Komerční banka a.s. (KB)**

Banka byla založena roku 1990 a nyní patří mezi čtyři největší banky v České republice, je mateřskou společností Skupiny KB a je členem francouzské Skupiny Société Générale. „*KB je univerzální bankou se širokou nabídkou služeb v oblasti retailového, podnikového a investičního bankovnictví.*“ [29] Dle hodnocení ze serveru Banky.cz patří KB mezi banky s průměrnými úroky hypoték i spotřebitelských úvěrů, účtuje si vysoké poplatky a nenabízí příliš velké zhodnocení peněz na spořicích účtech i termínovaných vkladech. Jako pozitivní hodnocení uvádí stabilitu banky na trhu a nabídku firemního bankovnictví s výhodnými produkty pro větší podniky. [30]

Banka nabízí tyto produkty: [30]

- Osobní účty
- Spořicí účty
- Spotřebitelské úvěry
- Termínované vklady
- Hypotéky
- Jistotní účty
- Stavební spoření
- Penzijní připojištění

4.1.4. **Československá obchodní banka a.s. (ČSOB)**

ČSOB byla založena státem v roce 1964 a nyní je stoprocentní dceřinou společností KBC Bank. V detailovém bankovnictví pod banku spadá ERA a Poštovní spořitelna. „*ČSOB poskytuje své služby všem klientským segmentům, tj. fyzickým osobám, malým a středním podnikům, korporátním a institucionálním klientům.*“ [31] ČSOB má v současné době více než 3 miliony klientů, z nichž více jak 1,3 milionů využívá Internetové bankovnictví. Provozuje 249 ČSOB poboček a 914 bankomatů. Klienti mohou využívat služeb na 73 pobočkách ERA a na zhruba 3200 obchodních místech České pošty. Server Finexpert hodnotí banku jako spolehlivou a zavedenou, poskytující plný rozsah služeb s největším počtem obchodních míst. Negativní hodnocení přidávají vyšší ceny služeb, drahé inkasní platby a neosobní přístup Poštovní spořitelny, neznalé bankovních služeb. [32]

Banka nabízí tyto produkty: [33]

- Osobní účty
- Spořicí účty
- Spotřebitelské úvěry
- Termínované vklady
- Hypotéky
- Jistotní účty
- Stavební spoření
- Penzijní připojištění
- Životní a úrazové pojištění
- Pojištění nemovitostí a domácnosti
- Cestovní pojištění a další pojištění

4.2. Uživatelská rozhraní vybraných bank

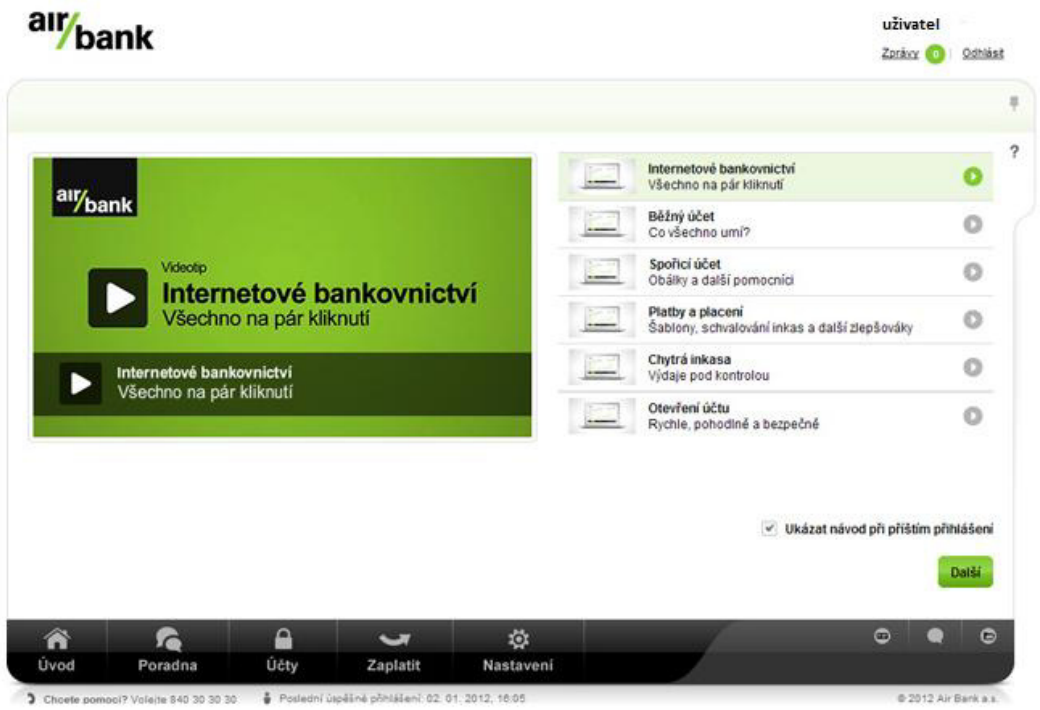
Uživatelská rozhraní jednotlivých bank se liší samozřejmě v grafickém provedení, ale také v přehlednosti jednotlivých produktů a nabídek a ve způsobu ovládání. Banky neustále zdokonalují svá Internetové bankovnictví, nabízejí stále více produktů dostupných prostřednictvím webového rozhraní, přizpůsobují rozhraní uživatelským nárokům, jednotlivé služby jsou zpoplatněny nižší sazbou než na pobočce. Banky tímto v podstatě usnadňují klientům komunikaci s bankou, šetří jejich čas a zároveň ulehčují práci sami sobě, operace zadávané prostřednictvím internetového bankovnictví jsou zpracovány automaticky a tím i snižují náklady na zaměstnance a provoz poboček.

4.2.1. **Air Bank a.s.**

Elektronické bankovnictví nabízí tyto služby:

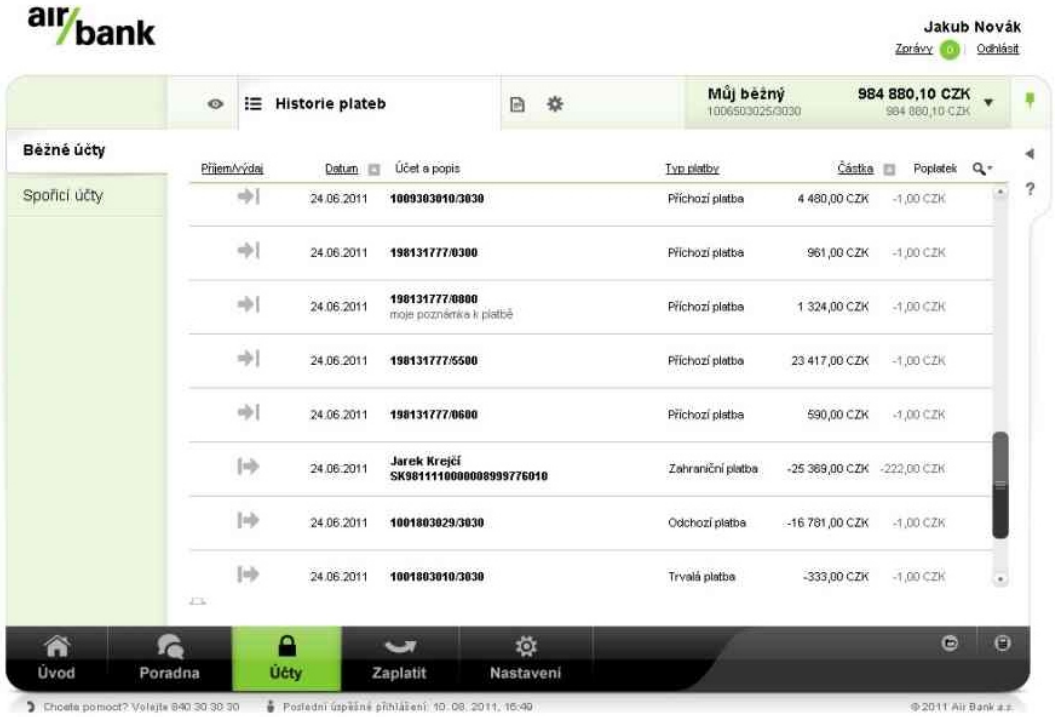
- Běžné bankovní činnosti (platby, inkaso, historie transakcí, elektronické výpisy).
- Změna limitů pro platby kartou a u obchodníka.
- Založení běžného účtu.
- Vystavení nové karty.
- Aktuální informace o všech účtech a produktech.
- Využití internetového bankovnictví jako e-mail.
- Přístup ke všem dokumentů mezi klientem a bankou.
- Grafické přehledy o příjmech a výdajích pro různá období.

Obrázek 2 – Hlavní strana IB Air Bank a.s.



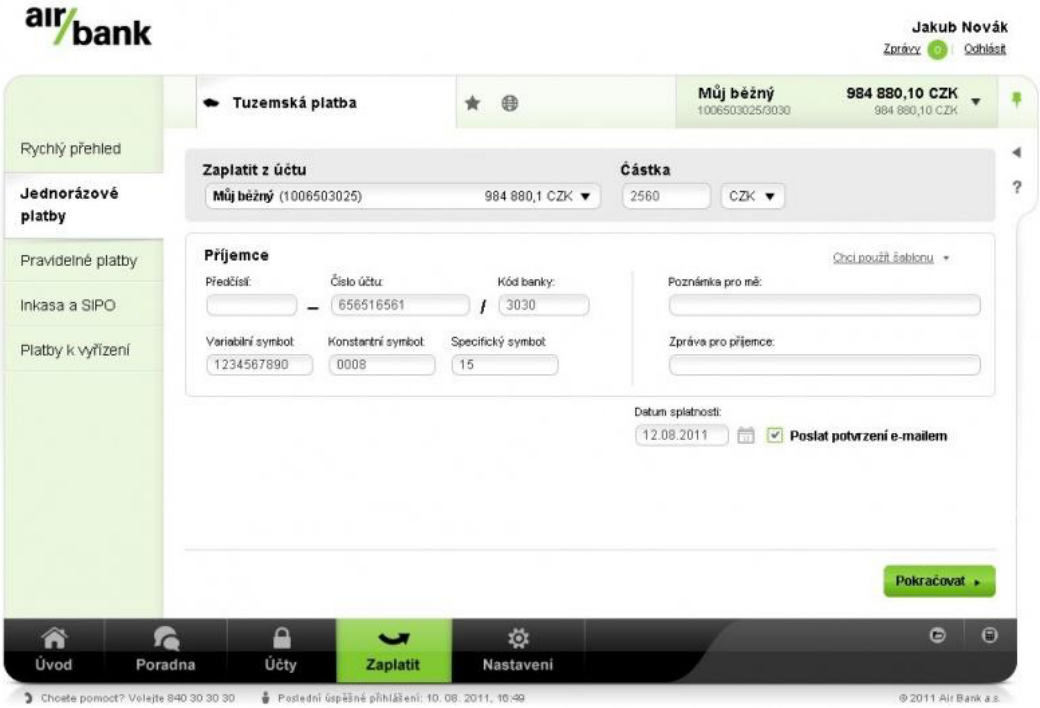
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://blog.filosof.biz/wp-content/uploads/2012/01/air1.jpg

Obrázek 3 – Historie transakcí Air Bank a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://js.pencdn.cz/Image.aspx?itemid=235156&width=&height=&q=100

Obrázek 4 – Jednorázová platba Air Bank a.s.



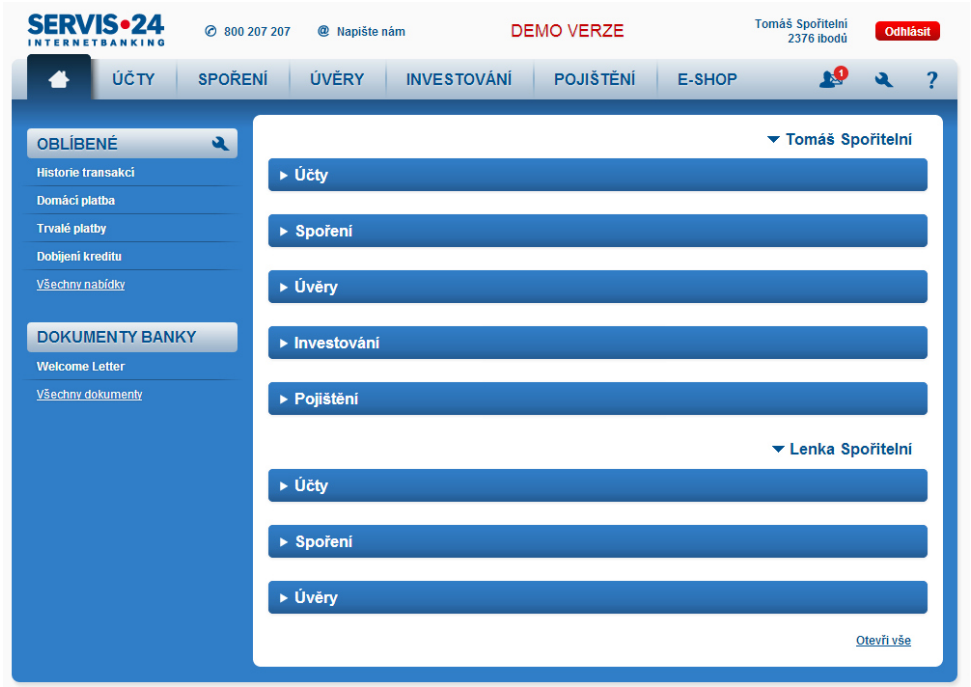
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.airbank.cz/cs/vse-o-air-bank/novinky/skutecne-internetove-bankovnictvi/Contents.2/2/48EAF12D0E3B39924E679DF1F210A06F/original.jpg?width=800

4.2.2. **Česká spořitelna a.s. (ČS)**

Elektronické bankovnictví nabízí tyto služby:

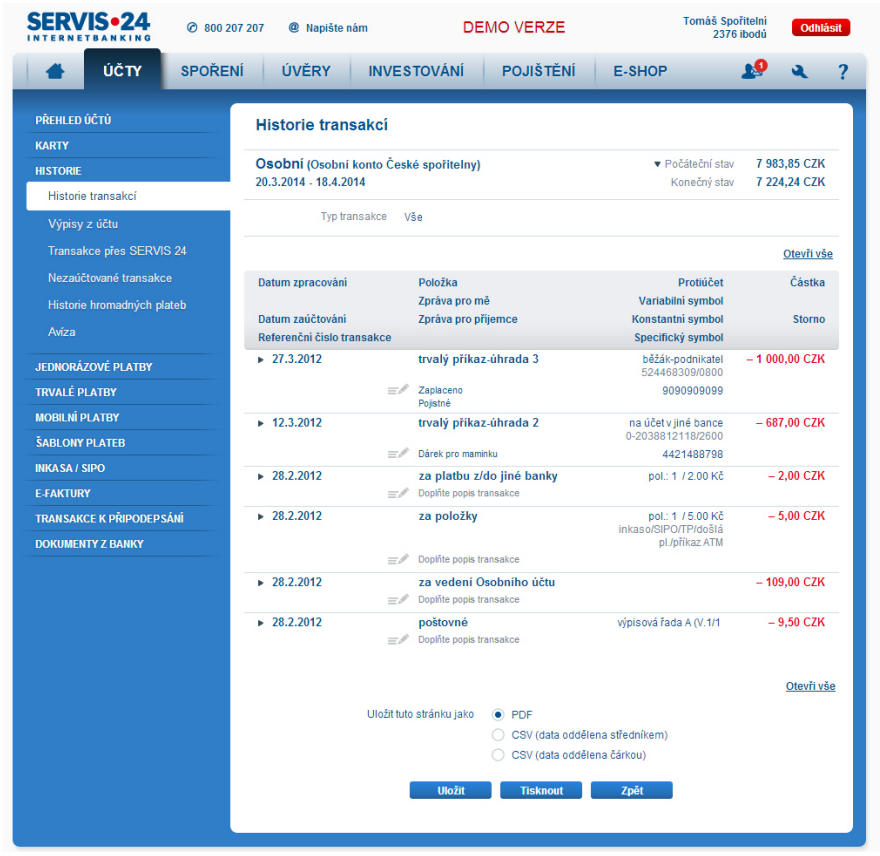
- Běžné bankovní činnosti (platby, inkaso, historie transakcí, elektronické výpisy).
- Aktuální informace o všech účtech a produktech.
- Úvěry - sjednání úvěru, kontokorentu nebo chytré karty.
- Dobití předplacené karty mobilních operátorů.
- Změna limitů pro platby kartou, na internetu a pro výběr v hotovosti v bankomatu.
- Nastavení parametrů karty či sjednání pojištění karty a osobních věcí.
- E-faktury – služba umožňuje přijímat a jednoduše platit faktury za služby, předpisy pojistného, složenky.
- Spoření – přehled, založení nového spoření.
- Investice – přehled, nákup a prodej investic.
- Přehled pojištění.

Obrázek 5 – Hlavní strana IB ČS a.s.



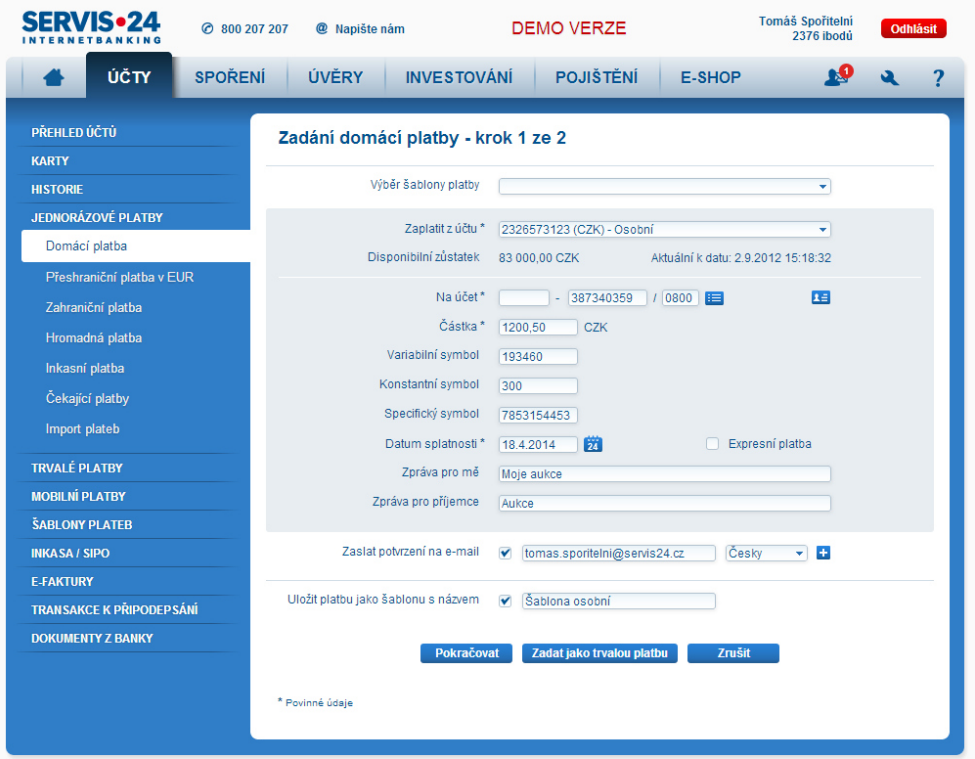
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.servis24.cz/demo-s24/ib/base/usr/aut/login ?execution=e1s1

Obrázek 6 – Historie transakcí ČS a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.servis24.cz/demo-s24/ib/base/usr/aut/login ?execution=e1s1

Obrázek 7 – Jednorázová platba ČS a.s.



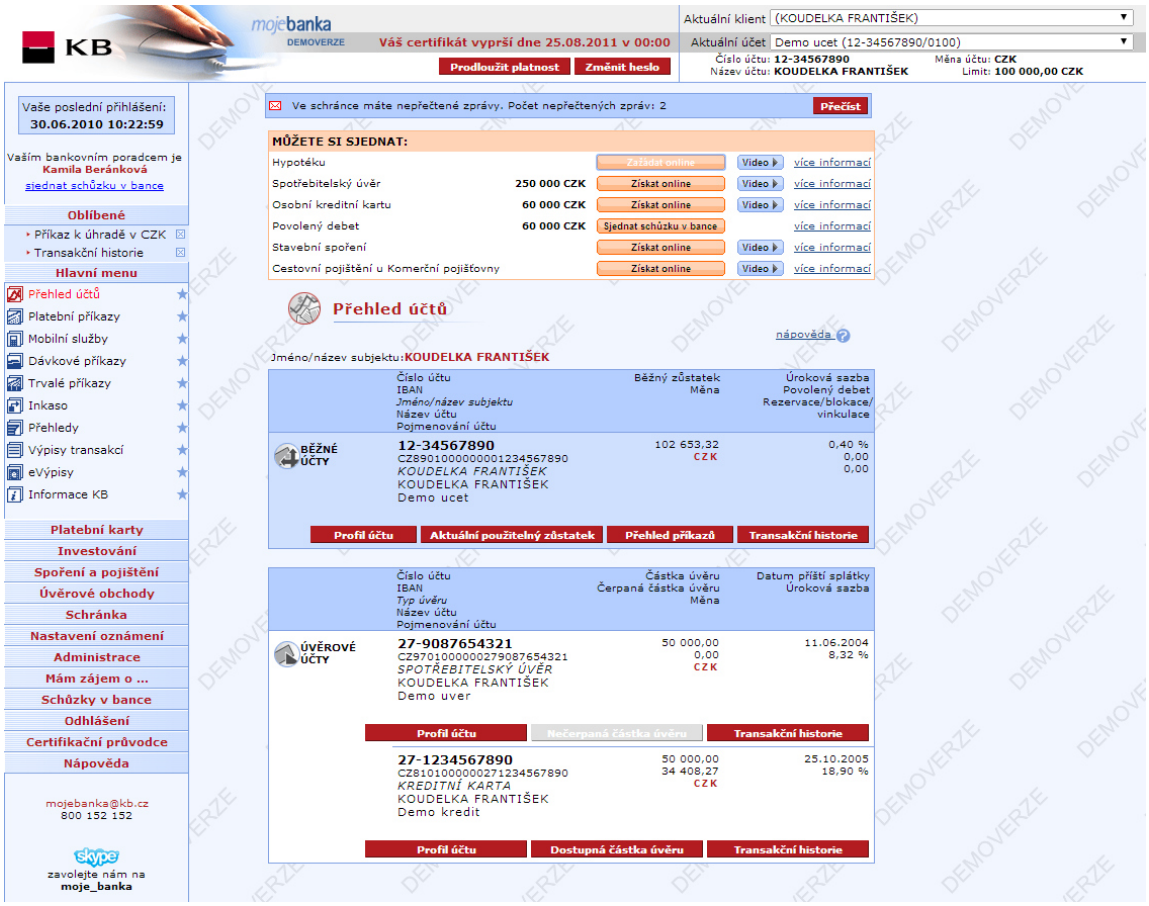
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.servis24.cz/demo-s24/ib/base/usr/aut/login ?execution=e1s1

4.2.3. **Komerční banka a.s. (KB)**

Elektronické bankovnictví nabízí tyto služby:

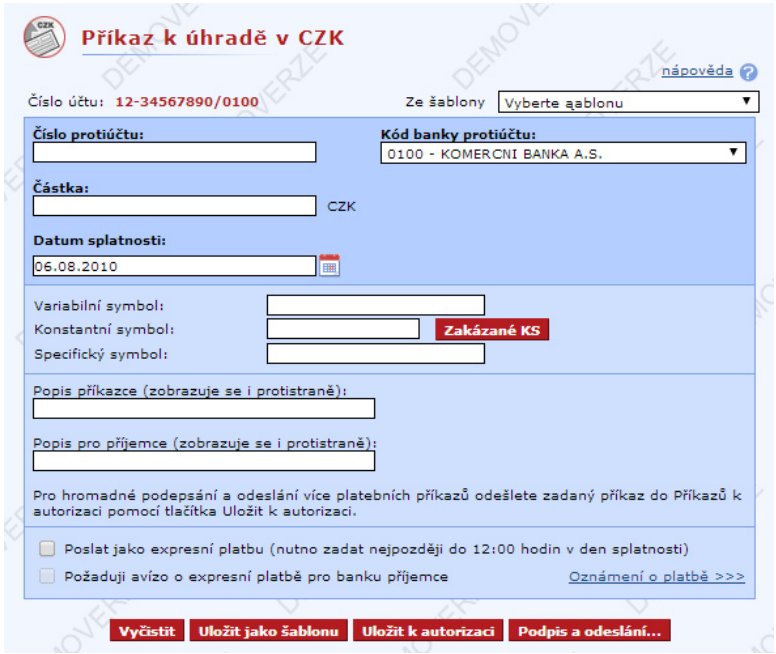
- Běžné bankovní činnosti (platby, inkaso, historie transakcí, elektronické výpisy).
- Aktuální informace o všech účtech a produktech.
- Zasílání informačních SMS a e-mailů.
- Úprava limitů platebních karet.
- Povolení a zablokování karet.
- Dobití předplacené karty mobilních operátorů.
- Přehled aktuálních dostupných úvěrových limitů pro možnost získání úvěru ihned.
- Spotřebitelské úvěry – přehled, sjednání nového úvěru.
- Hypotéky – přehled, uzavření nové hypotéky.
- Investice – přehled, založení nové investice.
- Uzavření cestovního pojištění.

Obrázek 8 – Hlavní strana IB KB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.mojebanka.cz/cs/demo/mb/cz/index.html

Obrázek 9 – Jednorázová platba KB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.mojebanka.cz/cs/demo/mb/cz/index.html

Obrázek 10 – Historie transakcí KB a.s.

Transakční historie

nápověda

Za období od 20.02.2007 do 06.03.2007 Rozšířený filtr

1 den | 5 dnů | 10 dnů | 15 dnů | pouze účetní transakce

Příkazy: všechny | Třídění dat dle: papírového výpisu

Stručný přehled | Tisk přes TXT | Vyčistit filtr | Zobrazit

Číslo účtu 12-345678901/ 0100 CZK

Zvolené období: od 26.01.2005 do 18.02.2005 | Počet příkazů: 8 | Vlastní číslo výpisu:

Obrat na vrub: 6 200,00 | Obrat ve prospěch: 34,74 | Počáteční zůstatek: 104 123,83 | Konečný zůstatek: 97 958,57

Číslo protiúčtu / Typ transakce / ID transakce	VS / KS / SS	Částka a měna	Datum přijetí k zaúčtování / Datum splatnosti / Datum zaúčtování
102463612/0300 Úhrada ID transakce	6737484119 3558 0	-152,00 CZK	18.02.2005 20.02.2005 18.02.2005
Popis příkazce :	1. RADEK POPISU		
Popis pro příjemce :	NA AC-0000000102463612		
Systémový popis:	Úhrada do jiné banky		
19553160257/0100 Úhrada ID transakce	6020015750 0 0	-5 000,00 CZK	02.02.2005 02.02.2005 02.02.2005
Popis příkazce :	IKS BALANCOVANY		
Systémový popis:	Platba na vrub vašeho účtu		
125784320/0300 Úhrada ID transakce	6823569028 3558 0	-762,00 CZK	01.02.2005 01.02.2005 01.02.2005
Popis příkazce :	1. RADEK POPISU		
Popis pro příjemce :	NA AC-0000000125784320		
Systémový popis:	Úhrada do jiné banky		
865285520247/0100 Úhrada ID transakce	9 558 0	-200,00 CZK	01.02.2005 01.02.2005 01.02.2005
Popis příkazce :	1. RADEK POPISU		
Popis pro příjemce :	NA CK-0000865285520247		
Systémový popis:	Platba na vrub vašeho účtu		
0/0100 Úhrada ID transakce	0 0 0	+34,74 CZK	31.01.2005 31.01.2005 31.01.2005
Popis příkazce :	PŘIPSANÝ ÚROK		
Systémový popis:	Připsaný úrok		

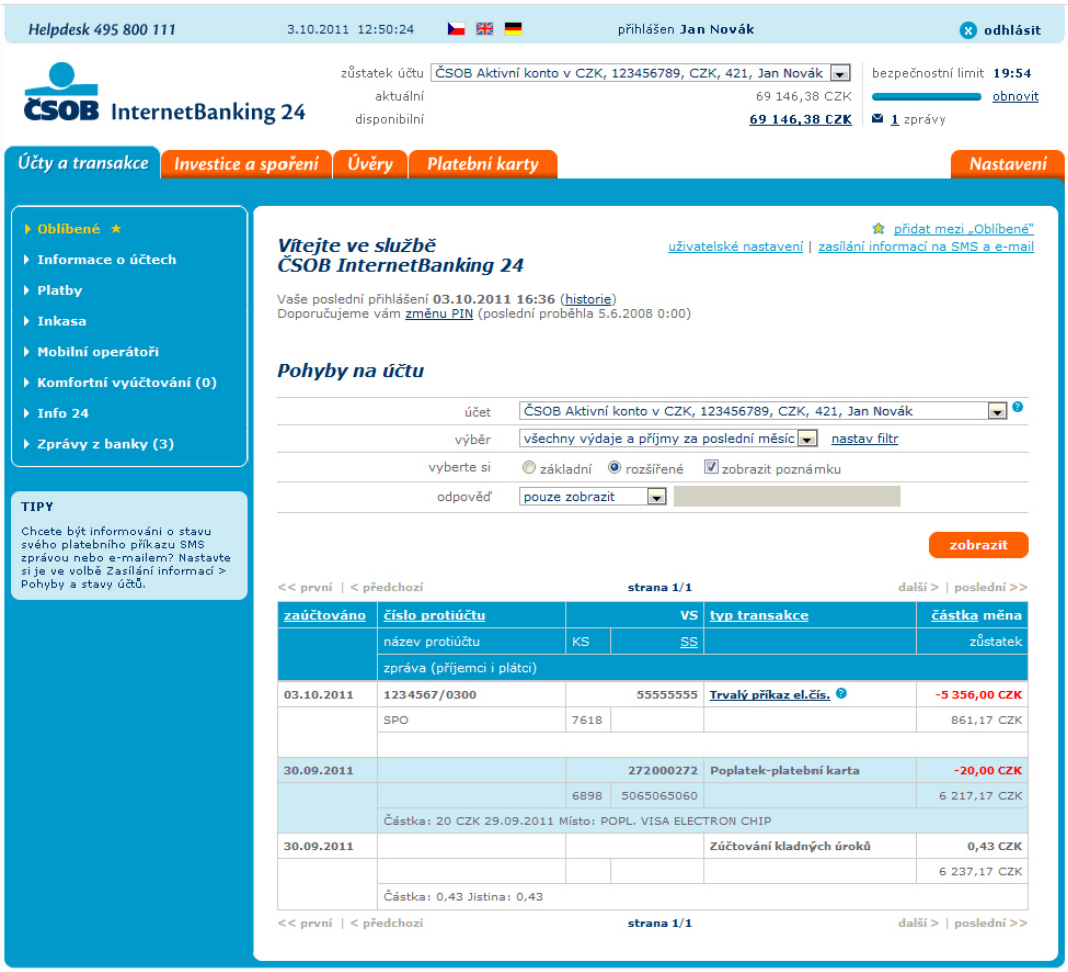
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.mojebanka.cz/cs/demo/mb/cz/index.html

4.2.4. Československá obchodní banka a.s. (ČSOB)

Elektronické bankovnictví nabízí tyto služby:

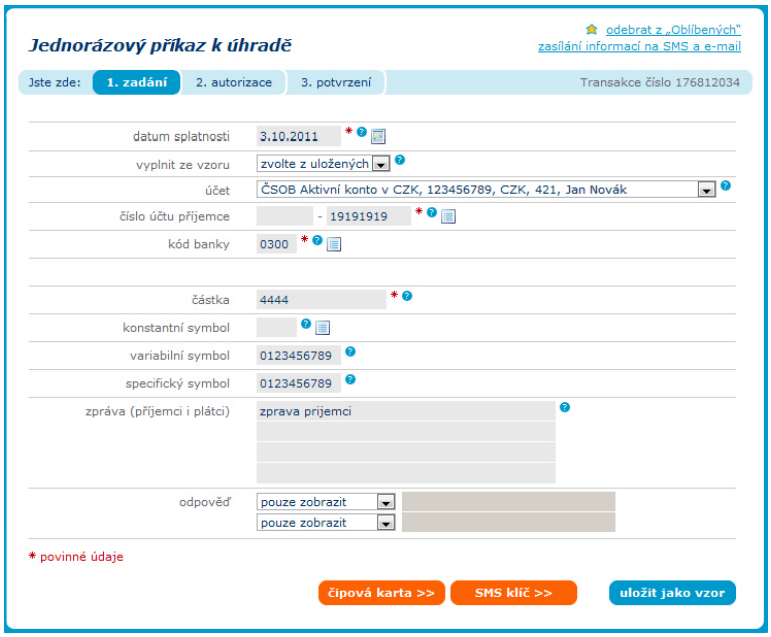
- Běžné bankovní činnosti (platby, inkaso, historie transakcí, elektronické výpisy).
- Žádosti o úvěry a jejich správa.
- Přehled o podílových fondech a investicích.
- Přehled penzijního připojištění.
- Přehled hypoték.
- Zasílání informačních SMS a e-mailů.
- Dobití předplacené karty mobilních operátorů.
- Spotřebitelské úvěry – přehled, sjednání nového úvěru.

Obrázek 11 – Hlavní strana IB a historie transakcí ČSOB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.csob.cz/WebCsob/Lide/Elektronicke-bankovnictvi/IB/Ukazky/IB24_demo_2011-11.swf

Obrázek 12 – Jednorázová platba ČSOB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.csob.cz/WebCsob/Lide/Elektronicke-bankovnictvi/IB/Ukazky/IB24_demo_2011-11.swf

4.3. Způsoby zabezpečení vybraných bank

V této kapitole jsou sepsány způsoby přihlašování do Internetových bankovnictví a vyobrazena přihlašovací webová rozhraní vybraných bank. Informace o přihlašování a zabezpečení bank jsou převzaté z oficiálních webů jednotlivých bank. Banky uvádí, jakým způsobem je možné se přihlásit do internetového bankovnictví, jakým způsobem probíhá komunikace mezi bankou a klientem a jakými metodami jsou chráněné vůči neoprávněným přístupům.

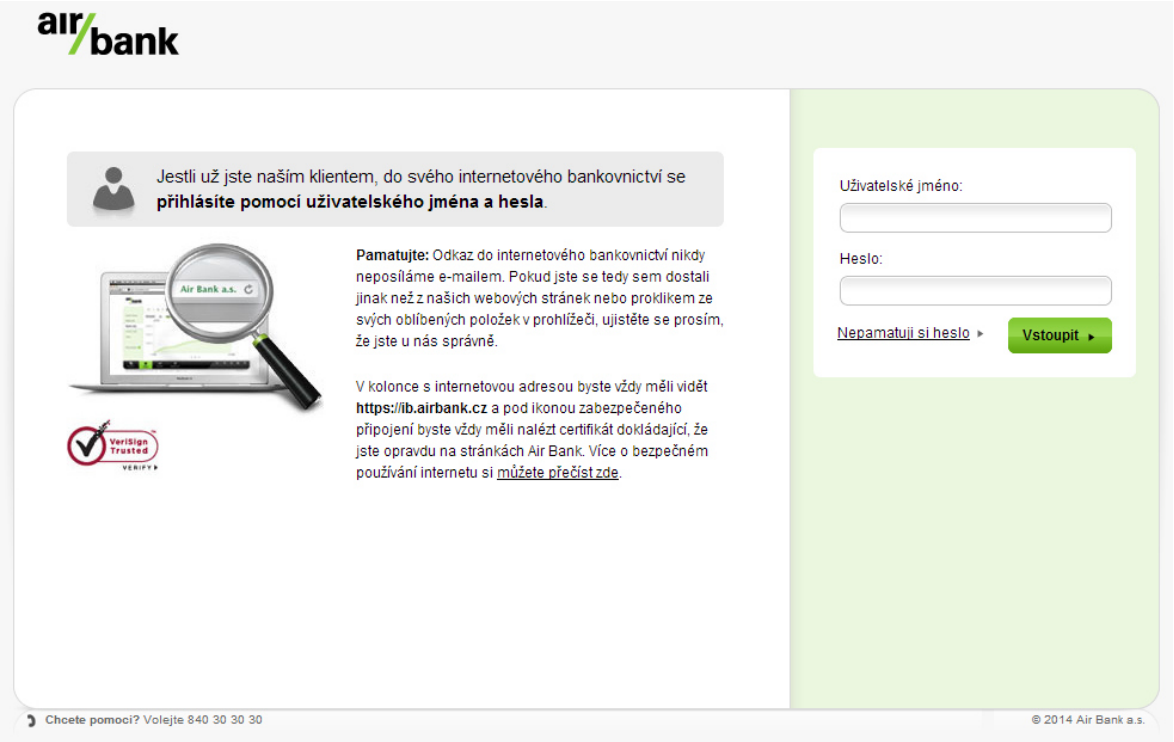
4.3.1. **Air Bank a.s.**

Banka nikdy nežádá po klientovi v elektronické komunikaci zaslání osobních dat, loginů a hesel, PINů, atd.

Internetové bankovnictví využívá protokolu HTTPS. Platnost stránky je ověřena certifikátem od mezinárodně uznávané certifikační autority Verisign. [34]

Konkrétnější informace týkající se zabezpečení banka na svých stránkách neuvádí.

Obrázek 13 – Přihlašovací rozhraní IB Air Bank a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://ib.airbank.cz/

4.3.2. Česká spořitelna a.s. (ČS)

Pro přihlášení do Internetového bankovnictví je vyžadováno klientské číslo a heslo, a klientský certifikát či přihlašovací SMS. Po správném zadání uvedených údajů a jejich ověření jste oprávněni užívat všechny pasivní operace. Všechny aktivní transakce je nutné dodatečně autorizovat pomocí autorizačního SMS kódu či klientského certifikátu.

Bezpečnost komunikace mezi bankou a klientem po internetu je zajištěna silným 128bitovým šifrováním pomocí technologie SSL. Pro navázání šifrované komunikace je navíc použit certifikát serveru banky vydaný důvěryhodnou certifikační autoritou. V závislosti na typu prohlížeče se v adresním řádku zobrazuje ikona zamčeného visacího zámku.

Banka je chráněna proti napadení svých systémů účinnou kombinací hardwarových a softwarových obranných prvků jako jsou firewally, detektory průniku nebo oddělením jednotlivých informačních systémů od přístupu z internetu. Účinnost těchto ochran je pravidelně kontrolována vzhledem k bezpečnostním politikám banky.

E-maily informující o změně zůstatků, elektronické výpisy a potvrzení bankou přijatých transakcích ve formátu PDF jsou zabezpečeny digitálním podpisem. [35]

Obrázek 14 – Přihlašovací rozhraní IB ČS a.s.

Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.servis24.cz/demo-s24/ib/base/usr/aut/login?execution=e1s1

4.3.3. **Komerční banka a.s. (KB)**

Přihlašování do Internetového bankovnictví je v první fázi řešeno pomocí osobního certifikátu s platností dva roky, který je klíčem pro autentizaci spojení mezi bankou a klientem. Po uložení certifikátu do zabezpečeného úložiště prohlížeče je důležité neukládat soubor na disk počítače, ale zálohovat jej na přenosné médium. Pro zvýšení bezpečnosti uložení Vašeho osobního certifikátu můžete využít čipové karty. Přihlášení do bankovnictví pokračuje zadáním jména a hesla a následného zadání autorizačního klíče z SMS.

Veškerá komunikace mezi bankou a klientem probíhá přes zabezpečený kanál SSL. Každou aktivní operaci uživatel potvrzuje svým elektronickým podpisem nebo autorizační SMS.

Komerční banka nikdy nepožaduje osobní údaje, hesla ani nezasílá nevyžádané e-maily s odkazy na internetové adresy. [36]

Obrázek 15 – Přihlašovací rozhraní IB KB a.s.

Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: http://www.mojebanka.cz/cs/demo/mb/cz/login.html

4.3.4. Československá obchodní banka a.s. (ČSOB)

Internetové bankovnictví ČSOB je rozděleno na BusinessBanking a InternetBanking. Jsou zde tři způsoby přihlašování. Prvním je Identifikační číslo a heslo pouze pro BusinessBanking. Další možností je Identifikační číslo, heslo a SMS klíč tvořící 9ti místný alfanumerický řetězec rozdělený do trojic znaků oddělených pomlčkou (např. asd-v1b-gh7) s platností 10 minut pro InternetBanking. [37] Při autorizaci SMS klíčem jsou k zasílání zpráv využívány šifrované nebo nešifrované SMS zprávy. [38] Poslední možností je přihlášení pomocí čipové karty s certifikátem platným na 1 rok a potvrzováním operací pomocí PINu. [37] „*ČSOB vydává certifikát TWINS, který obsahuje certifikát komerční i kvalifikovaný. Komerčním certifikátem se přihlašujete do služby a kvalifikovaným autorizujete transakce.*“ [37] Veškerá komunikace mezi klientem a bankou probíhá šifrovaně.

Obrázek 16 – Přihlašovací rozhraní IB ČSOB a.s.

Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://ib24.csob.cz/

4.4. Test zabezpečení vybraných bank pomocí online SSL Server Test

Na základě informací o vybraných bankách jsem se rozhodl jejich zabezpečení otestovat pomocí online služby „SSL Server Test", kterou bezplatně poskytuje společnost Qualys Inc. na webové stránce https://www.ssllabs.com/ssltest/ . Tato služba provádí hloubkovou analýzu konfigurace na libovolném webovém serveru SSL ve veřejné síti SSL. Společnost Qualys Inc. dále poskytuje službu „SSL Klient Test", umožňující otestovat zabezpečení Vašeho webového prohlížeče.

Společnost QUALYS Inc.

Společnost byla založena v roce 1999 a navázala strategické partnerství s předními poskytovateli řízených služeb a poradenských organizací, včetně BT, Dell, SecureWorks,

Fujitsu, IBM a dalšími. Společnost je také zakládajícím členem Cloud Security Alliance (CSA). Qualys Inc. je přední poskytovatel informační bezpečnosti a dodržování Cloud Solutions. QualysGuard Cloud Platform a integrovaná sada řešení pomáhá podnikům zjednodušit bezpečnostní operace a snížit náklady na dodržování předpisů o poskytování kritické bezpečnostní informace, automatizaci v celém bezpečnostním provozu a ochranu IT systémů a webových aplikací. QualysGuard ® služba používá dnes více než 6700 společností ve více než 100 zemích. [39]

SSL Server Test

Bezplatný online SSL Test zkoumá SSL certifikát webové stránky, aby bylo jasné, zda je důvěryhodný a slouží jako základ pro zabezpečenou komunikaci přes internet. Provádí také komplexní analýzu ke zjištění konfigurace zabezpečení, jeho slabin a problémů s výkonem. Výsledky testů zahrnují číselné skóre od 0 do 100 roztříděné do několika kategorií.

Pomocí SSL testu každý uživatel, ať už technicky zdatný či nikoliv, dostane zhodnocení o kvalitě zabezpečení zadané webové stránky a může se rozhodnout, či bude stránce důvěřovat, nebo ne, a tím se chránit před možnými útoky nebo ztrátě citlivých údajů. [40]

"SSL je úspěšný protokol, který slouží jako bezpečnostní páteř internetu, ale na většině míst ho nemají dobře nastavený," [40] řekl Ivan Ristic, ředitel techniky pro Qualys a tvůrce SSL Labs.

Metodika testu

1. Ověření certifikátu, zda je platný a důvěryhodný.
2. Kontrola konfigurace serveru ve třech kategoriích.
   2.1. Podpora protokolu.
   2.2. Podpora výměny klíčů.
   2.3. Síla šifry.
3. Sloučení a vyhodnocení skóre.
   3.1. Jednotlivé kategorie vyhodnoceny v intervalu od 0 do 100.
   3.2. Celkové vyhodnocení pomocí tabulky:

Tabulka 2 – Kritéria pro vyhodnocení SSL Server Testu

score >= 80 … A
score >= 65 … B
score >= 50 … C
score >= 35 … D
score >= 20 … E
score < 20 ….. F

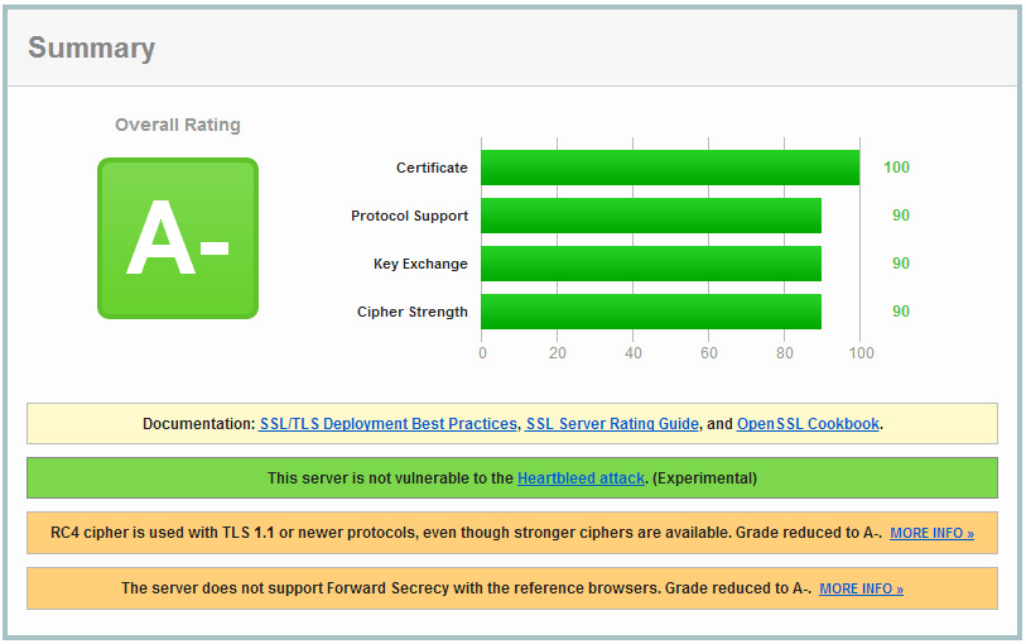
Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009e.pdf

4. Uplatnění série pravidel pro zjištění aspektů serverů, které nelze vyjádřit numericky. Ty poté snižují konečné skóre. Třída A- ukazuje na servery s obecně dobrou konfigurací, které mají jeden nebo více upozornění. Třída A+ ukazuje na servery s výjimečně dobrou konfigurací, bez varování a striktním transportním protokolem HTTP platným po dobu 6 měsíců.

4.4.1. **Grafické vyhodnocení SSL Server Testu**

Air Bank a.s.

Obrázek 17 – Výsledek SSL Server testu pro Ari Bank a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=ib.airbank.cz

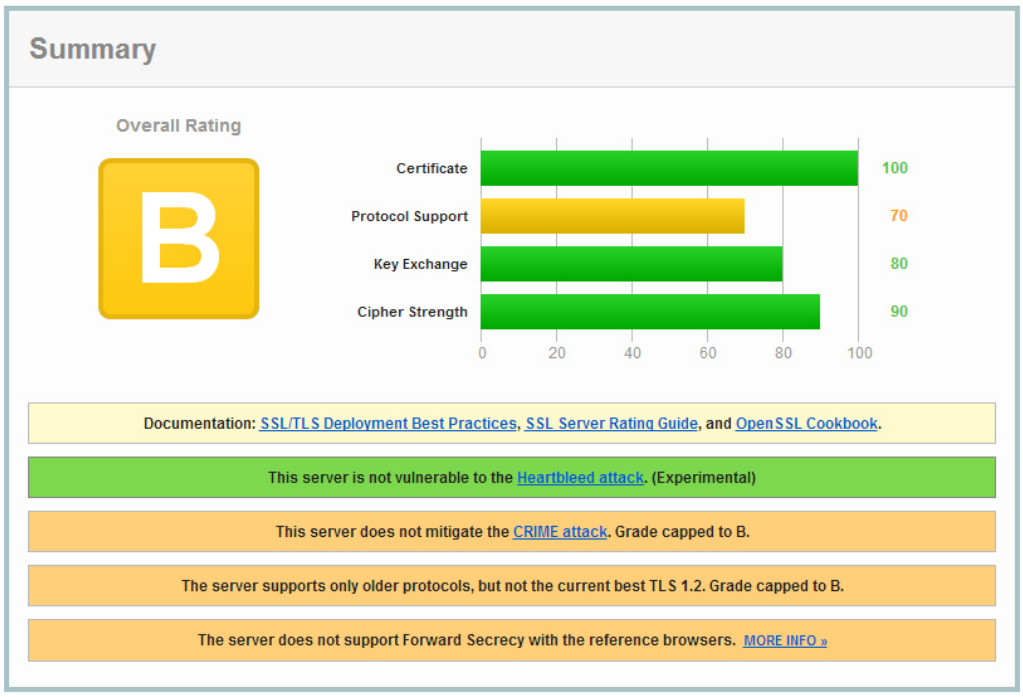
Tento server není náchylný k útoku Heartbleed .

RC4 šifra se používá s TLS 1.1 či novějšími protokoly, ale k dispozici jsou i silnější šifry, proto stupeň snížen na A-.

Server nepodporuje Forward Secrecy s referenčními prohlížeči. Stupeň snížen na A-.

Česká spořitelna a.s.

Obrázek 18 – Výsledek SSL Server testu pro ČS a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=servis24.cz

Tento server není náchylný k útoku Heartbleed .

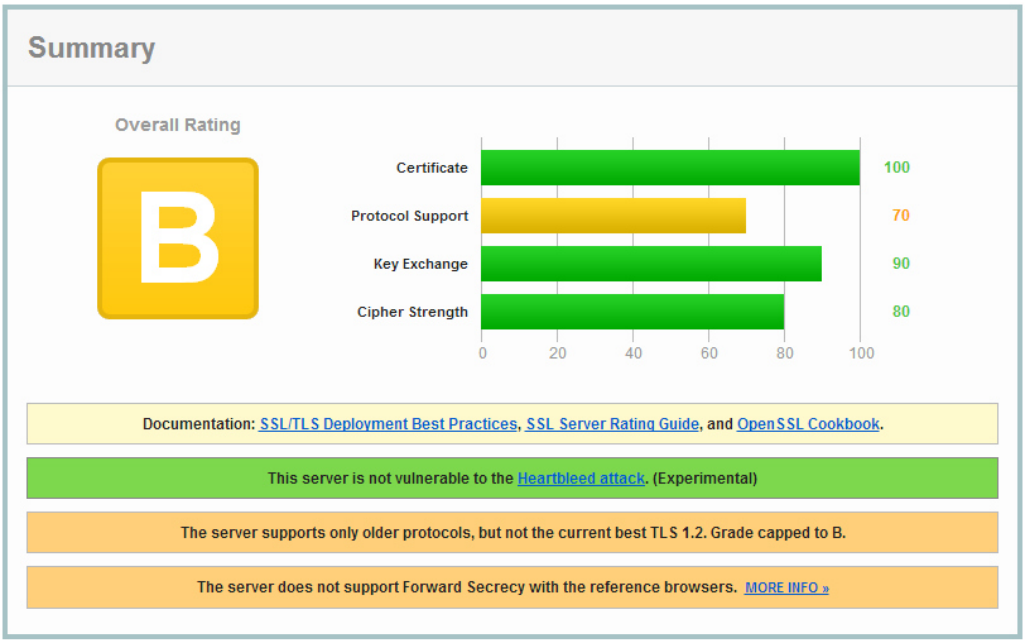
Tento server je náchylný k útoku na kompresi dat před šifrováním. Stupeň snížen na B.

Server podporuje pouze starší protokoly, ale ne aktuální nejlepší TLS 1.2. Stupeň snížen na B.

Server nepodporuje Forward Secrecy s referenčními prohlížeči.

Komerční banka a.s.

Obrázek 19 – Výsledek SSL Server testu pro KB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=mojebanka.cz

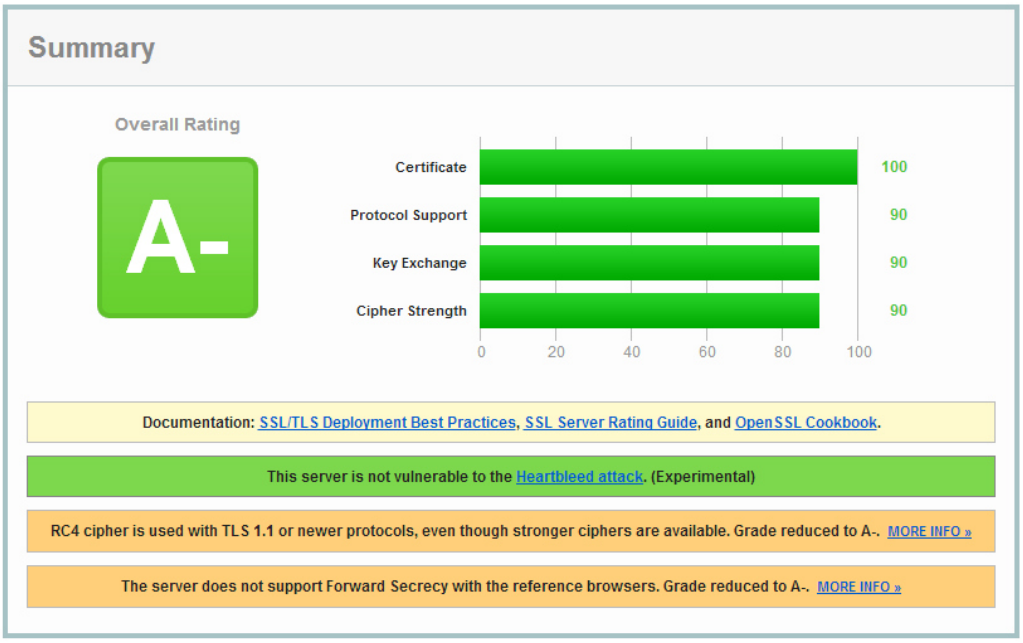
Tento server není náchylný k útoku Heartbleed .

Server podporuje pouze starší protokoly, ale ne aktuální nejlepší TLS 1.2. Stupeň snížen na B.

Server nepodporuje Forward Secrecy s referenčními prohlížeči.

Československá obchodní banka a.s.

Obrázek 20 – Výsledek SSL Server testu pro ČSOB a.s.



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=ib24.csob.cz

Tento server není náchylný k útoku Heartbleed .

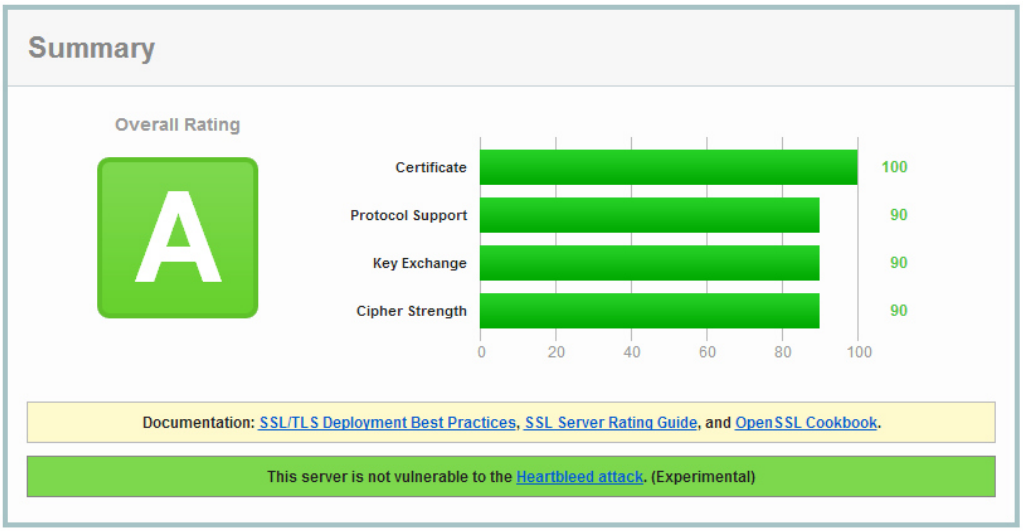
RC4 šifra se používá s TLS 1.1 či novějšími protokoly, ale k dispozici jsou i silnější šifry, proto stupeň snížen na A-.

Server nepodporuje Forward Secrecy s referenčními prohlížeči. Stupeň snížen na A-.

Zabezpečení serveru Google.com

Hodnocení SSL Server Testu pro server Google.com je zde uvedeno pro srovnání s výsledky testů Internetových bankovnictví.

Obrázek 21 – Výsledek SSL Server testu pro Google.com



Zdroj: [online]. [cit. 2014-04-13]. Dostupné z: https://www.ssllabs.com/ssltest/analyze.html?d=google.com

Tento server není náchylný k útoku Heartbleed .

4.4.2. **Komplexní porovnání výsledků provedeného SSL Server Testu**

Tabulka 3 – Porovnání výsledků SSL Server Testu

	Air Bank	**ČS**	**KB**	**ČSOB**	**Google**
Hodnocení	A-	B	B	A-	A
Certifikat					
Klíč	RSA 2048 bitů	RSA 2048 bitů	RSA 2048 bits	RSA 2048 bitů	RSA 2048 bitů
Certifikační autorita	VeriSign Class 3 Extended Validation SSL SGC CA	VeriSign Class 3 Extended Validation SSL SGC CA	VeriSign Class 3 Extended Validation SSL SGC CA	GlobalSign Extended Validation CA - G2	Google Internet Authority G2
Algoritmus podpisu	SHA1withRSA	SHA1withRSA	SHA1withRSA	SHA1withRSA	SHA1withRSA
Důvěryhodnost	Ano	Ano	Ano	Ano	Ano
Protokol					
Typy	SSL 3 TLS 1.0 TLS 1.2	SSL 3 TLS 1.0	SSL 3 TLS 1.0	SSL 3 TLS 1.0 TLS 1.2	SSL 3 TLS 1.0 TLS 1.1 TLS 1.2
Bezpečné opětovné projednání	Ano	Ano	Ano	Ano	Ano
Klientem započaté opětovné projednání	Ne	Ne	Ne	**Ne, hrozba DoS**	Ne
Komprese TSL	Ne	**Ano nežádoucí**	Ne	Ne	Ne
RC4	Ano (s TLS 1.1 a novějšími) nežádoucí	Ano (ne TLS 1.1 a novější)	Ano (ne TLS 1.1 a novější)	Ano (s TLS 1.1 a novějšími) nežádoucí	Ano (ne TLS 1.1 a novější)
Heardbleed	Ne	Ne	Ne	Ne	Ne
Session resumption	Ano	**Ne (ID přiřazeno, ale není přijato)**	**Ne (ID prázdný)**	Ano	Ano
Forward Secrecy	Ne, nežádoucí	Ne, nežádoucí	Ne, nežádoucí	Ne, nežádoucí	Ano s moderními prohlížeče

Zdroj: vlastní zpracování

Vysvětlivky k tabulce:

Bezpečné opětovné projednání - SSL a TLS umožňují dojednání funkcí zabezpečeného spojení opětovně projednat.

Klientem započaté opětovné projednání - Opětovné projednání směrované ze strany uživatele není žádoucí, hrozí útoky typu *Denial of Service* (DoS).

Komprese TLS - Více v kapitole 1.5.3.

RC4 - Šifrovací sada RC4 je považována za nejistou a by měla být zakázána.

Session resumption (relace obnovení) - umožňuje opětovné použití nedávno platného Session ticket (lístku relace) pro obnovení relace, užívá se pro optimalizaci výkonu

Forward Secrecy - Je to proces, během něhož obě strany interpretují své schopnosti na druhou stranu, provádějí ověřování a dojednávají klíče relace. Ty se pak používají k zašifrování zbytku relace. Cílem výměny klíčů je umožnit oběma stranám vyjednat klíče bezpečně. Existuje několik mechanizmů výměny klíčů. V tuto chvíli se nejčastěji používá metoda založená na RSA, kde soukromý klíč serveru slouží k ochraně klíče relace. To je efektivní přístup, ale kdokoli s přístupem na kopii soukromého klíče serveru může odhalit klíče relace a dešifrovat rozhovor. Alternativou je použití Diffie-Hellman algoritmu, který je pomalejší, ale generuje klíče relace takovým způsobem, že třetí osoba tyto klíče získat nemůže a to ani v případě, že mají přístup k soukromému klíči na serveru. [41]

4.4.3. Vyhodnocení provedeného testu

Na základě provedeného SLS Server Testu lze konstatovat, že z vybraných bank v testu nejlépe vyhověly Air Bank a.s. a Československá obchodní banka a.s., jejich hodnocení je A-. Česká spořitelna a.s. a Komerční banka a.s. získaly v testu hodnocení B. V tabulce jsou zaznamenané základní informace o certifikátech a vybrané informace o protokolech, rozšířené o nedostatky v zabezpečení. Protože jsou výsledky testů příliš rozsáhlé, nejsou zde uvedeny všechny. Kompletní výsledky testů jsou dostupné z webových stránek SSL Server Testu.

Z výsledků testů Internetových bankovnictví vybraných bank je patrné, že:

- Využívají důvěryhodnou certifikační autoritu, stejný algoritmus podpisu SHA1with RSA a klíč certifikátu RSA 2048bitů.
- Ani jedno IB vybraných bank nepodporuje nedůvěryhodný protokol SSL 2 a IB ČS a.s. a KB a.s. nepodporují novější transportní protokoly TLS 1.1 a TLS 1.2.
- Umožňují bezpečné opětovné projednání klíčů, nežádoucí opětovné projednání směrované ze strany klienta je umožněno u IB ČSOB a.s. (hrozba útoku typu DoS).
- Nežádoucí kompresi TLS umožňuje IB ČS a.s. (hrozba útoku typu MITM).
- Šifru RC4, která je nežádoucí pro protokoly TLS 1.1 a novější, umožňuje Air Bank a.s. a ČSOB a.s., druhé dvě banky protokoly TLS 1.1 a novější vůbec nepodporují.
- Žádné z IB vybraných bank neumožňují útoky typu Heardbleed.
- IB ČS a.s. a KB a.s. mají problémy s přihlášením ke službě Session resumption.
- Využití protokolu Forward Secrecy nepodporuje ani jedno IB vybraných bank.

Porovnání se serverem Google.com:

- Získal v testu nejlepší hodnocení, známka A.
- Podporuje protokoly SSL3, TLS 1.0, TLS 1.1 a TLS 1.2.
- Není napadnutelný útoky typu DoS, Heardbleed, MITM a útoky na kompresy TLS.
- Šifra RC4 není použitelná pro protokoly novější TLS 1.1.
- Umožňuje využití protokolu Forward Secrecy, ale pouze s prohlížeči, které to podporují (aktuálně Google Chrome, Mozilla Firefox).

Kompletní výsledky testů dostupné z:

Air Bank a.s. - https://www.ssllabs.com/ssltest/analyze.html?d=ib.airbank.cz

Česká spořitelna a.s. - https://www.ssllabs.com/ssltest/analyze.html?d=servis24.cz

Komerční banka a.s. - https://www.ssllabs.com/ssltest/analyze.html?d=mojebanka.cz

ČSOB a.s. - https://www.ssllabs.com/ssltest/analyze.html?d=ib24.csob.cz

Google - https://www.ssllabs.com/ssltest/analyze.html?d=google.com

4.5. Průzkum trhnu: Využívání Internetového bankovnictví

Za účelem zjištění informací o veřejném mínění, týkající se Internetového bankovnictví, jsem vytvořil anonymní anketu s názvem: „Používáte Internetové bankovnictví, a pokud ano, jste s ním spokojen?“. Průzkum byl prováděn v Liberci a jeho blízkém okolí dotazníkovou metodou, elektronickou formou pomocí sociálních sítí a e-mailů, a písemnou formou dotazováním v ulicích. Do cílové skupiny dotazovaných patří převážně mladí lidé od 15 do 40 ti let. Ankety se zúčastnilo celkem 92 respondentů.

Výsledky dotazníku

1. Kolik Vám je let?

Tabulka 4 – Výsledky dotazníku k otázce 1.

15 – 26	43
27 – 40	28
41 – 60	14
Více než 60	7

Zdroj: vlastní zpracování

2. Vaše profese?

Tabulka 5 – Výsledky dotazníku k otázce 2.

Student	29
Dělník	18
Technik	23
Úředník	16
Důchodce	6

Zdroj: vlastní zpracování

3. Vaše nejvyšší dosažené vzdělání?

Tabulka 6 – Výsledky dotazníku k otázce 3.

Základní	4
Střední odborné bez maturity	15
Střední odborné s maturitou	31
Vyšší odborné	7
Vysokoškolské Bc.	19
Vysokoškolské Ing., Mgr.	13
Vysokoškolské vyšší	3

Zdroj: vlastní zpracování

4. Máte bankovní účet?

Tabulka 7 – Výsledky dotazníku k otázce 4.

ANO	81
NE	11

Zdroj: vlastní zpracování

5. Jakou využíváte banku?

Tabulka 8 – Výsledky dotazníku k otázce 5.

Česká Spořitelna	30
Komerční Banka	11
ČSOB	17
AirBank	8
GE Money Bank	6
Era	2
mBank	4
Raiffeisenbank	3

Zdroj: vlastní zpracování

6. Používáte Internetové bankovnictví?

Tabulka 9 – Výsledky dotazníku k otázce 6.

ANO	58
NE	23

Zdroj: vlastní zpracování

7. Přijde Vám jako jednoduché, dostupné a spolehlivé?

Tabulka 10 – Výsledky dotazníku k otázce 7.

ANO	37
ČÁSTEČNĚ	16
NE	5

Zdroj: vlastní zpracování

8. Jaký typ zabezpečení využíváte?

Tabulka 11 – Výsledky dotazníku k otázce 8.

Jméno a heslo	14
Jméno, heslo a SMS klíč	21
Jméno, heslo, certifikát a SMS klíč	19
Jméno, heslo, certifikát a PIN kalkulátor	3
Jméno, heslo, certifikát a biometrie	1

Zdroj: vlastní zpracování

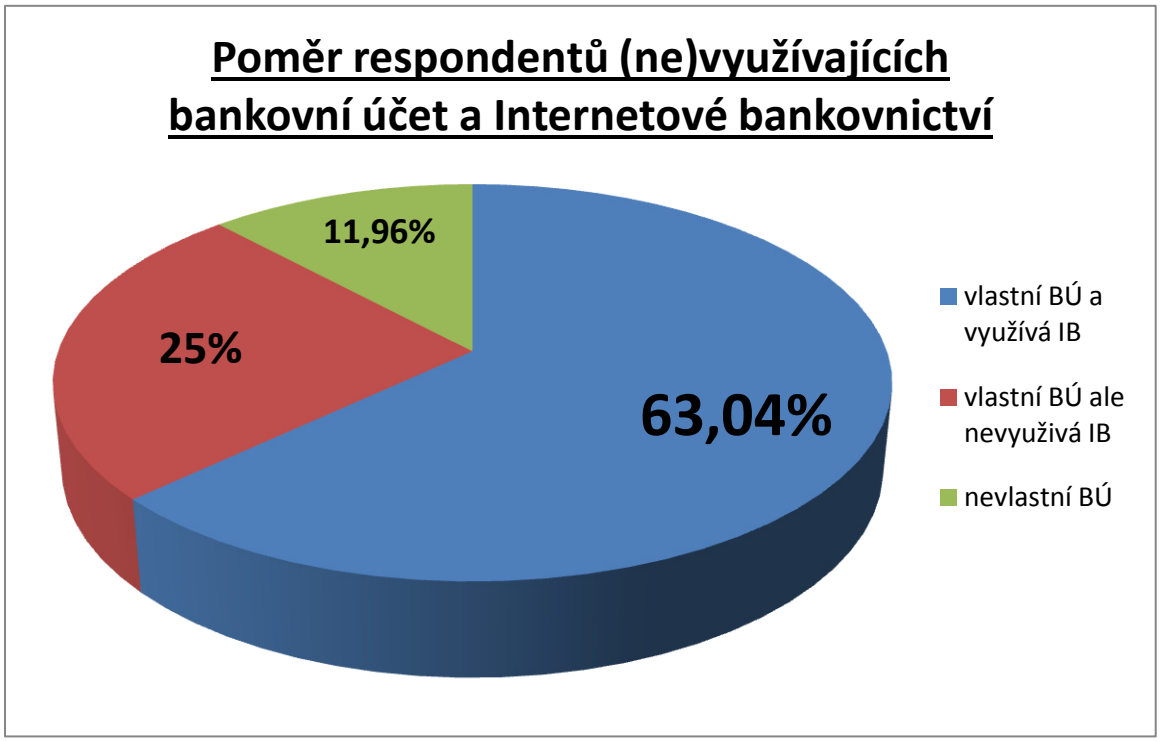
9. Přijde Vám způsob zabezpečení dostatečný?

Tabulka 12 – Výsledky dotazníku k otázce 9.

ANO	30
ČÁSTEČNĚ	21
NE	7

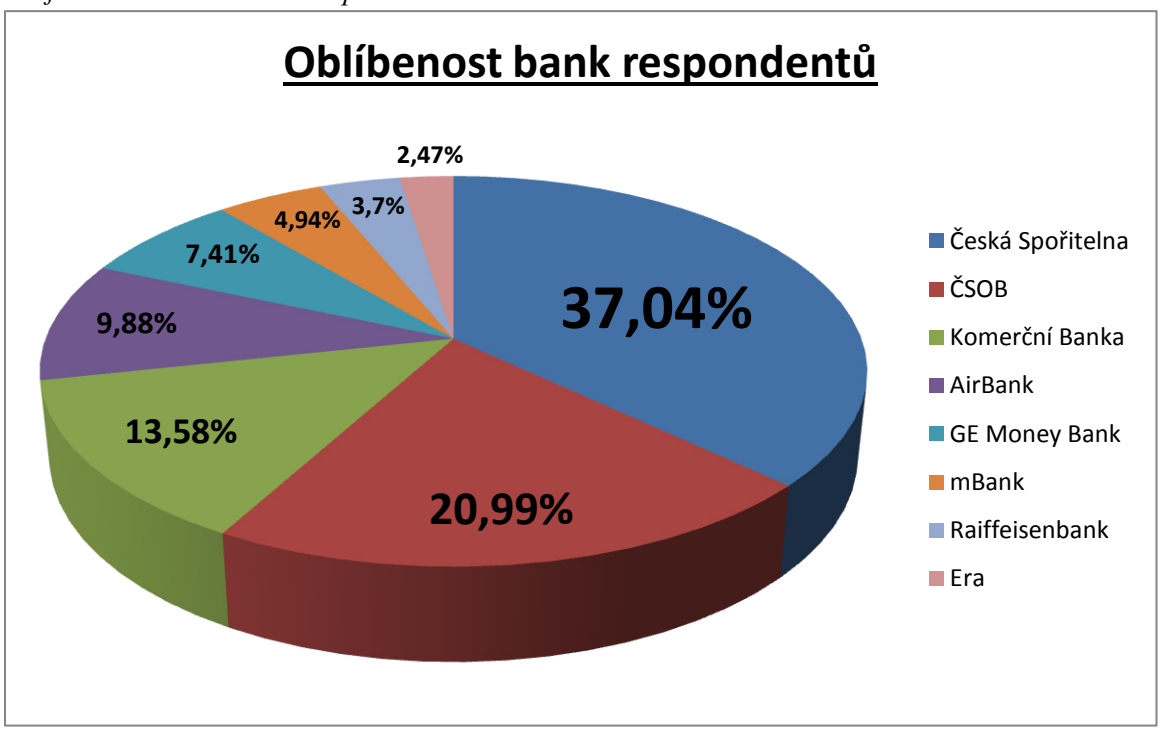
Zdroj: vlastní zpracování

Graf 4 – Poměr respondentů (ne)využívající bankovní účet a Internetové bankovnictví



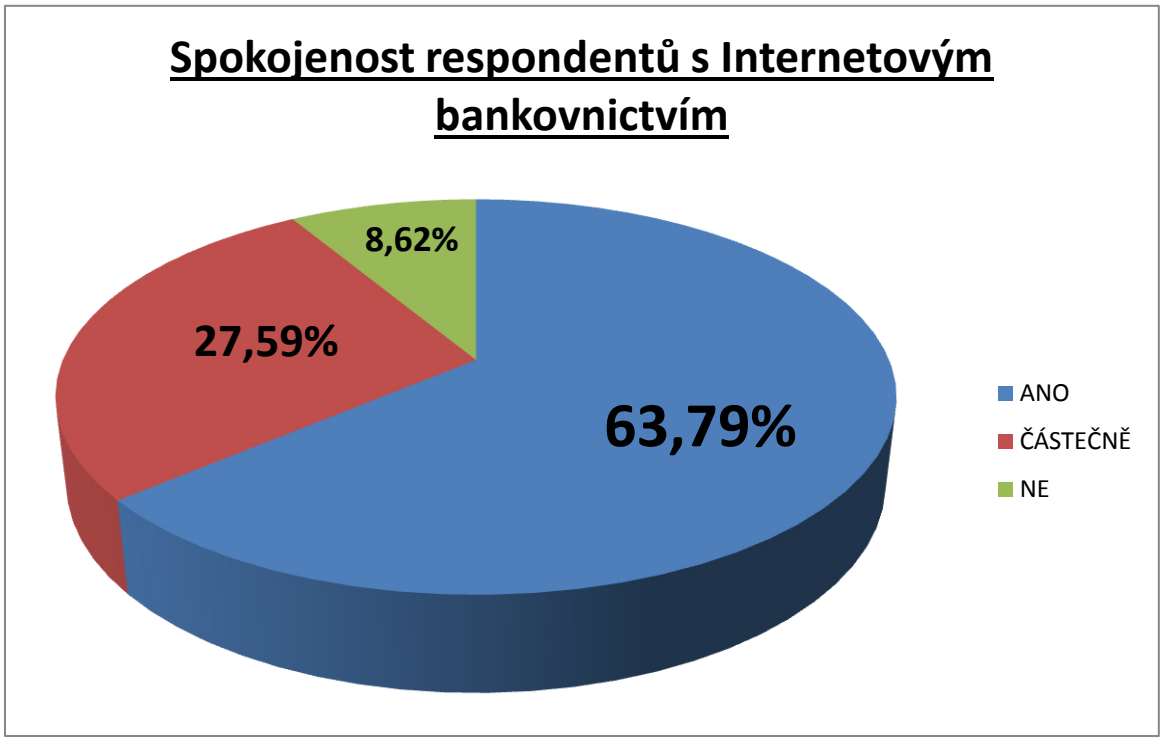
Zdroj: vlastní zpracování

Graf 5 – Oblíbenost bank respondentů



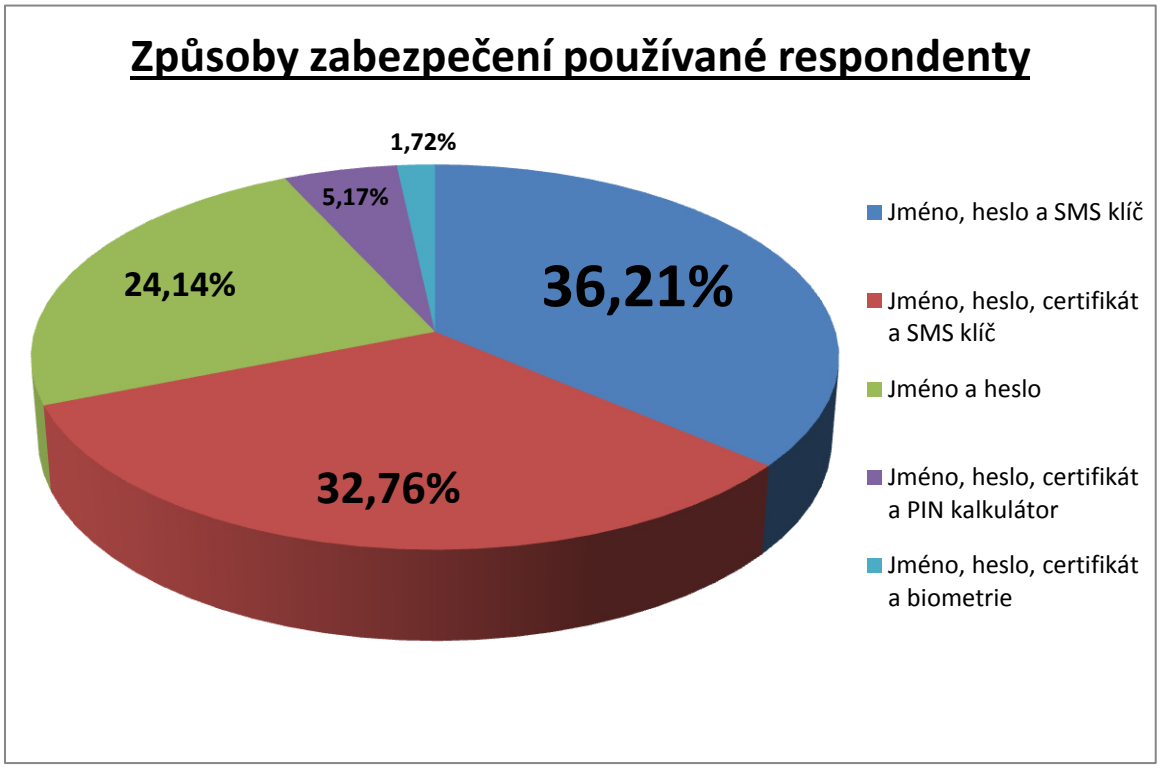
Zdroj: vlastní zpracování

Graf 6 – Spokojenost respondentů s Internetovým bankovnictvím



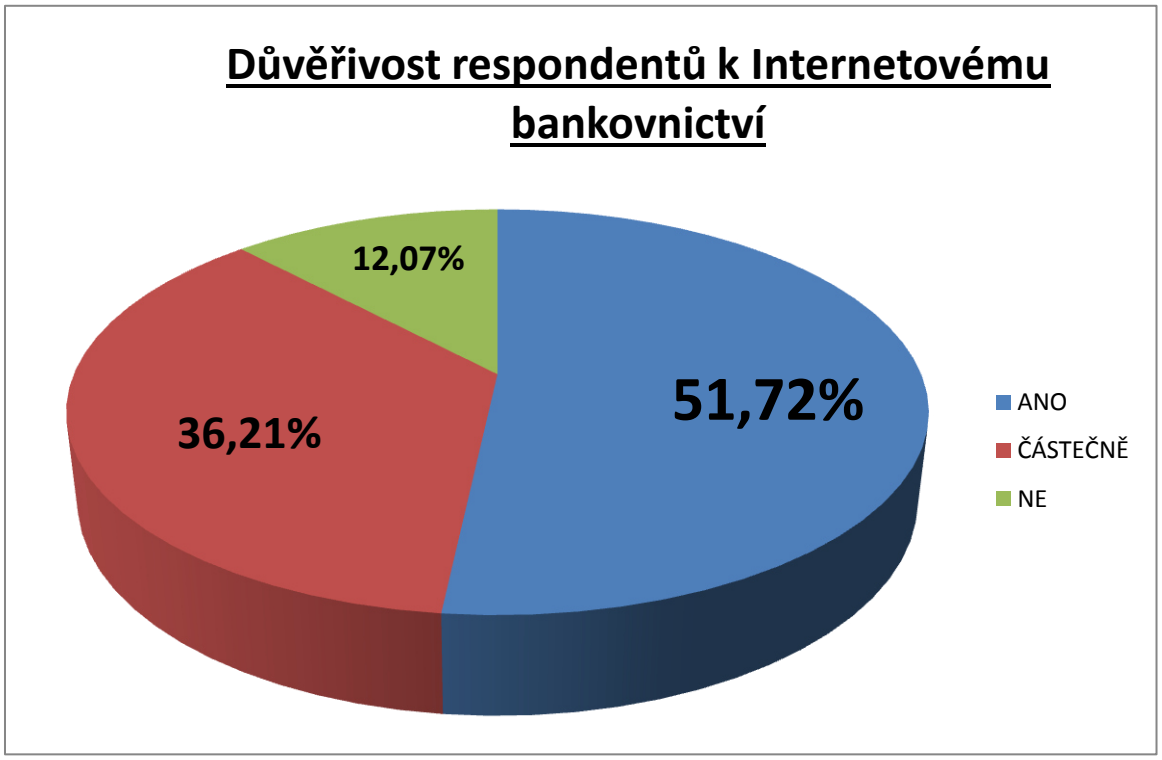
Zdroj: vlastní zpracování

Graf 7 – Způsoby zabezpečení používané respondenty



Zdroj: vlastní zpracování

Graf 8 – Důvěřivost respondentů k Internetovému bankovnictví



Zdroj: vlastní zpracování

Shrnutí výsledků ankety

Z provedené ankety, které se zúčastnilo 92 respondentů, vyplývají tyto závěry:

- Bankovní účet má a zároveň využívá Internetové bankovnictví 63% respondentů.
- Mezi tři nejoblíbenější banky patří Česká spořitelna a.s. (37%), Československá obchodní banka a.s. (21%) a Komerční banka a.s. (14%).
- S Internetovým bankovnictvím je spokojeno téměř 64% respondentů.
- Nejčastějším způsobem zabezpečení, které respondenti využívají k přihlášení do Internetového bankovnictví je: jméno, heslo a SMS klíč (36%), následuje jméno, heslo, certifikát a SMS klíč (33%) a dále jenom jméno a heslo (24%).
- Internetovému bankovnictví věří pouze necelých 52% respondentů.

5. Doporučení pro minimalizaci možných ohrožení (pro různé skupiny uživatelů)

V této části uvádím základní pravidla počítačové bezpečnosti. Protože těchto pravidel je nepřeberné množství, vybral jsem jen ty nejzákladnější a detailně jsem uvedl především pravidla, týkající se bezpečného používání internetového bankovnictví. Pravidla pro bezpečné používání počítače, pohybu v síti a zabezpečení komunikace uvádí i každý server Internetového bankovnictví, popsaný v této práci.

Server Bezpečný internet.cz rozděluje skupinu uživatelů na začínající uživatele, pokročilé uživatele, rodiče a děti. Ke každé skupině uživatelů jsou sepsány zásady bezpečnosti pro nejčastější operace s počítačem.

O projektu Bezpečný Internet

„Projekt Bezpečný internet.cz oslovuje různé cílové skupiny uživatelů a na názorných příkladech pomáhá vytvářet správné návyky internetové bezpečnosti. Projekt není vázán na produkty žádných společností a zcela zdarma poskytuje rady, návody i zkušenosti provozovatelů nejnavštěvovanějších internetových služeb.“ [42]

5.1. Začínající uživatelé

Pro začínající skupinu uživatelů se zásadní otázky bezpečnosti týkají především procházením webových stránek, zabezpečení online komunikace, ochrany osobních údajů, rady jak se chovat na sociálních sítích, jak volit hesla, jak bezpečně používat e-mail a jak správně zabezpečit osobní počítač. Uvádím jen některé z nich:

Hesla

Aby heslo plnilo svoji funkci, je třeba zvolit dostatečně silné heslo a dodržovat pravidla práce s ním. Síla hesla je určena několika faktory:

- Délkou, pro běžná hesla se používá 8 – 14 znaků.
- Složením, mělo by vypadat jako náhodný řetězec znaků.
- Mělo by obsahovat písmena malá i velká, číslice a nestandardní znaky.

Je důležité, aby Vaše heslo zůstalo tajné, není důvod, aby ho někdo měl znát, nemělo by být ani nikde napsáno nebo uloženo na disku počítače. Zároveň by heslo mělo být pravidelně měněno. Hesla používající pro přihlašování k různým serverům jsou přenášena po síti a hrozí nebezpečí jeho odposlechnutí. Interval pro změnu hesla by tedy měl být kratší, než např. heslo do osobního počítače, které po síti přenášeno není. Hesla je vhodné po určitém čase měnit. „Doba platnosti hesla by měla být tím kratší, čím je pro Vás důležitější to, co heslo chrání.“ [43]

Zabezpečení počítače

Dodržováním zásad zabezpečení osobního počítače uživatel snižuje riziko ztráty citlivých informací, které mohou být užity k následné trestné činnosti. Mezi tyto zásady patří:

- Antivirová ochrana – každý počítač by měl být vybaven antivirovým programem, který chrání před viry, červy a jiným nežádoucím softwarem. Zároveň by měl být pravidelně aktualizován.
- Brána Firewall – pracuje na principu filtru mezi osobním počítačem a internetem v obousměrné komunikaci, blokuje tedy útoky přicházející zvenčí, ale i programy pokoušející se o spojení zevnitř.
- Pravidelná aktualizace – aktualizace opravují chyby programů a bezpečností mezery, které by se daly použít pro neoprávněný přístup k datům, proto je doporučeno pravidelně aktualizovat operační systém, nainstalované programy i webové prohlížeče a jejich doplňky.
- Odstranění škodlivého software – může jím být Spyware, Adware, či jiný nežádoucí software pokoušející se o získání citlivých informací, nebo jen zahlcující systémovou paměť. Tento software je třeba z počítače odstranit. Programy pro odstraňování škodlivého software by měli být pravidelně aktualizovány. [44]

Bezpečný e-mail

Prostřednictvím e-mailů probíhá značná část celosvětové komunikace, ať už se jedná o obchodní nabídky a poptávky, sdělení či osobní zprávy, a je tedy i dalším místem útoku hackerů. Útočník se snaží vylákat z oběti citlivé údaje pomocí e-mailových zpráv označovaných jako SPAM. „Principem těchto zpráv je věrohodné napodobení oficiální žádosti banky nebo podobné instituce a vynutit si od adresáta jeho přihlašovací údaje na odkazované stránce.“ Hlavní zásadou bezpečného e-mailu je neotevírat přílohy zpráv, které přišly z neznámé adresy. [45]

5.2. Pokročilí uživatelé

Pokročilí uživatelé se pohybují po širším spektru internetové sítě a jejich nároky na bezpečnost v síti jsou vyšší. Server Bezpečný internet.cz popisuje způsoby jak chránit svá data, čeho se vyvarovat při stahování souborů z internetu, jak bezpečně používat Internetové bankovnictví, nakupovat online a jak se pohybovat ve veřejných sítích a na veřejných počítačích.

Veřejné sítě, veřejné počítače

Pokud jste připojeni k internetu na veřejném místě, např. v kavárně nebo na letišti, není bezpečné zadávat platební transakce, komunikace by mohla být zachycena útočníkem.

Na veřejných počítačích je důležité vždy se odhlásit před ochodem z webové stránky a nikdy neukládat své přihlašovací údaje do prohlížečů. Nepracujte s citlivými informacemi a smažte po sobě historii navštívených stránek a stažené soubory.

Stahování souborů z internetu

Je dobré mít na vědomí, že součástí stažených souborů může být i špionážní software, nebo volně stažitelný program může obsahovat nežádoucí kódy, které mohou infikovat Váš počítač. Vždy by jste si měli být jisti, zda stahovaný soubor pochází z důvěryhodného zdroje a zda

jeho použitím neporušujete autorská práva. „Při stahování programů, filmů, hudby a dalších souborů, k nimž se vážou autorská práva, je nutné zajistit dodržování těchto práv.“

Server uvádí rizika spojená s používáním nelegálního softwaru:

- Riziko trestního postihu za používání nelegálního softwaru.
- Riziko ztráty dat.
- Riziko virové nákazy počítače.
- Riziko finanční ztráty.
- Riziko ztráty soukromí.
- Riziko nemožnosti aplikovat bezpečnostní a funkční aktualizace.

Bezpečnost internetového bankovnictví

Pro zajištění bezpečnosti internetového bankovnictví je nutné dodržovat tyto zásady:

- Při přihlašování na účet internetového bankovnictví zkontrolovat, zda je spojení řádně zabezpečeno a zda skutečně komunikujete s Vaší bankou. Jestliže si nejste jisti, obraťte se na klientskou linku.
- Chraňte své elektronické údaje, hesla, PINy a ostatní informace.
- Dávejte pozor, zda potvrzujete Vámi zadanou transakci.
- Pravidelně kontrolujte pohyb na svých účtech.
- Finanční služby využívejte pouze z důvěryhodného a řádně zabezpečeného počítače.
- Na počítači, ze kterého používáte finanční služby, nepoužívejte a neinstalujte nedůvěryhodný software, nenavštěvujte nedůvěryhodné webové stránky a neotvírejte podezřelé poštovní zprávy. [46]

5.3. Rodiče

Projekt Bezpečný internet uvádí rady pro rodiče, jakým způsobem ochránit své děti před nástrahami internetu a ukazuje možnosti jak regulovat obsah zpřístupněný dětem.

- Umístěte počítač do místnosti používané celou rodinou.
- Mluvte o internetu.
- Naučte se lépe pracovat s počítačem.
- Používejte internet společně.
- Vytvořte s dětmi dohodu o tom, jak a kdy budou internet používat.

Je důležité, aby rodiče měli přehled o tom, jaké stránky jejich děti navštěvují, tím mohou zamezit možné kybernetické šikaně.

5.4. Děti

Server Bezpečný internet uvádí desatero bezpečnostních zásad formulovaných pro děti, jakým způsobem by se měli na internetu chovat a čeho se mají vyvarovat:

1. Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem na druhé straně.
2. Neposílej nikomu, koho neznáš, svou fotografii a už vůbec ne intimní. Svou intimní fotku neposílej ani kamarádovi nebo kamarádce - nikdy nevíš, co s ní může někdy udělat.
3. Udržuj hesla (k e-mailu i jiné) v tajnosti, nesděluj je ani blízkému kamarádovi.
4. Nikdy neodpovídej na neslušné, hrubé nebo vulgární maily a vzkazy. Ignoruj je.
5. Nedomlouvej si schůzku přes internet, aniž bys o tom řekl někomu jinému.
6. Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.
7. Svěř se dospělému, pokud tě stránky nebo něčí vzkazy uvedou do rozpaků, nebo tě dokonce vyděsí.
8. Nedej šanci virům. Neotevírej přílohu zprávy, která přišla z neznámé adresy.
9. Nevěř každé informaci, kterou na internetu získáš.
10. Když se s někým nechceš bavit, nebav se. [47]

Závěr

Internetové bankovnictví je jednou z vymožeností současné moderní doby, které pomáhá lidem při spravování jejich bankovních účtů prakticky z jakéhokoli místa na světě. Internetové bankovnictví však také může být bezpečnostním rizikem pro jejich uživatele, a to zejména při neznalosti možností zabezpečení a bezpečnostních pravidlech jeho používání.

V této bakalářské práci jsem se proto snažil poukázat na přednosti a hrozby související s Internetovým bankovnictvím. V teoretické části této práce je podrobně popsán postup komunikace klienta s bankou, nejčastější typy prolomení bezpečnosti, způsoby přihlašování do Internetového bankovnictví a technologie jeho zabezpečení. Praktická část obsahuje analýzu čtyř vybraných bank, které na území České republiky poskytují Internetové bankovnictví, z hlediska používaných certifikátů a zabezpečení komunikačních protokolů.

Analýza zabezpečení vybraných bank byla provedena pomocí SSL Server Testu, na základě kterého bylo zjištěno, že tyto banky používají stejný a bezpečný algoritmus podpisu certifikátu, který je vydaný důvěryhodnou certifikační autoritou. Test však prokázal, že některé Internetové bankovnictví vybraných bank nepodporují nejnovější komunikační protokoly, které zajišťují bezpečnou komunikaci. Nepoužíváním nejnovějších komunikačních protokolů, zejména v bankovním sektoru, může způsobit i odcizení finančních prostředků.

V praktické části bakalářské práce je také zhodnocena mnou provedená anketa se zaměřením na využívání a bezpečnost Internetového bankovnictví. Nejznepokojivějším výsledkem ankety je, že pouhých 52% respondentů považuje Internetové bankovnictví za bezpečné.

V poslední části této práce jsou uvedeny zásady a doporučení pro minimalizaci možných ohrožení pro různé skupiny uživatelů. Z výsledků mnou provedené ankety lze usoudit, že tyto zásady a doporučení pravděpodobně nejsou mezi uživateli Internetového bankovnictví obecně známé nebo nepoužívané.

Doporučením z provedeného testu zabezpečení Internetového bankovnictví vybraných bank je, aby banky pro minimalizaci možného ohrožení Internetového bankovnictví používaly nejnovější protokol typu TLS 1.2 a servery bank podporovaly Forward Secrecy.

Závěrem této bakalářské práce lze konstatovat, že Internetové bankovnictví je výhodný způsob komunikace klienta s jeho bankou, a při dodržování doporučení, uvedených v této bakalářské práci, je možné minimalizovat bezpečnostní rizika související s jeho používáním.

Seznam použité literatury

[1] PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví. Vyd. 1. Praha: Computer Press, 2000, 166 s. ISBN 80-7226-328-5.

[2] [online]. [cit. 2014-04-07]. Dostupné z: http://www.finance.cz/zpravy/finance/319968-jak-moc-se-pouziva-internetove-bankovnictvi-ve-svete-/

[3] [online]. [cit. 2014-04-07]. Dostupné z: http://www.ucetnikavarna.cz/archiv/dokument/doc-d9466v12332-elektronicke-bankovnictvi-2-cast/

[4] [online]. [cit. 2014-04-07]. Dostupné z: http://www.feedit.cz/wordpress/2014/04/02/studie-kaspersky-lab-rhybarum-jde-cim-dal-vic-o-penize-i-v-cesku

[5] [online]. [cit. 2014-04-24]. Dostupné z: http://heartbleed.com/

[6] [online]. [cit. 2014-04-24]. Dostupné z: http://www.zive.cz/bleskovky/polopate-jak-funguje-chyba-heartbleed-bug/sc-4-a-173264/default.aspx

[7] [online]. [cit. 2014-04-24]. Dostupné z: https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls

[8] [online]. [cit. 2014-04-24]. Dostupné z: https://community.qualys.com/blogs/securitylabs/2009/11/05/ssl-and-tls-authentication-gap-vulnerability-discovered

[9] [online]. [cit. 2014-04-10]. Dostupné z: http://informatika.topsid.com/index.php?war=prenosova_media_datovych_siti&unit=referencni_modely

[10] PUŽMANOVÁ, Rita a Jan KALA. TCP/IP v kostce. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.

[11] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5

[12] [online]. [cit. 2014-04-13]. Dostupné z: http://www.dsl.cz/jak-na-to/5-site-a-ochrana/232-jak-na-ssh

[13] [online]. [cit. 2014-04-13]. Dostupné z: http://www.root.cz/clanky/jak-nahradit-ftp-pomoci-sftp-a-zamknout-uzivatele/

[14] [online]. [cit. 2014-04-13]. Dostupné z: http://www.root-server.cz/korenove-servery.html

[15] [online]. [cit. 2014-04-14]. Dostupné z: http://earchiv.chip.cz/cs/earchiv/vydani/r-2008/internetove-bankovnictvi-kde-je-bezpecne.html

[16] [online]. [cit. 2014-04-014]. Dostupné z: http://genmedia.cz/blog/bezpecnost-internetoveho-bankovnictvi.html

[17] [online]. [cit. 2014-04-14]. Dostupné z: http://bankovnictvi.ihned.cz/c1-57223180-biometrie-a-elektronicke-podpisy

[18] [online]. [cit. 2014-04-15]. Dostupné z: http://finparada.cz/1749-Biometrie-metoda-autentizace-v-bankovnictvi.aspx

[19] [online]. [cit. 2014-04-15]. Dostupné z: http://business.center.cz/business/pravo/zakony/epodpis/cast1.aspx

[20] [online]. [cit. 2014-04-15]. Dostupné z: http://www.soom.cz/clanky/1126--Symetricke-a-asymetricke-sifrovani

[21] [online]. [cit. 2014-04-15]. Dostupné z: http://www.kryptografie.wz.cz/data/RSA.htm

[22] [online]. [cit. 2014-04-15]. Dostupné z: http://dml.cz/bitstream/handle/10338.dmlcz/141305/PokrokyMFA_51-2006-2_1.pdf

[23] [online]. [cit. 2014-04-15]. Dostupné z: http://www.earchiv.cz/b03/b0800001.php3

[24] [online]. [cit. 2014-04-15]. Dostupné z: http://computerworld.cz/securityworld/aplikacni-firewall-se-neomezuje-na-porty-a-protokoly-45322

[25] [online]. [cit. 2014-04-19]. Dostupné z: http://www.mesec.cz/clanky/deset-lakadel-kterymi-si-vas-chce-air-bank-ziskat/

[26] [online]. [cit. 2014-04-19]. Dostupné z: https://www.airbank.cz/cs/vse-o-air-bank/kdo-jsme/historie/

[27] [online]. [cit. 2014-04-19]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/profil-ceske-sporitelny-d00014413

[28] [online]. [cit. 2014-04-19]. Dostupné z: http://www.banky.cz/ceska-sporitelna

[29] [online]. [cit. 2014-04-19]. Dostupné z: https://www.kb.cz/cs/o-bance/o-nas/zakladni-informace.shtml

[30] [online]. [cit. 2014-04-19]. Dostupné z: http://www.banky.cz/komercni-banka

[31] [online]. [cit. 2014-04-19]. Dostupné z: http://www.csob.cz/cz/Csob/O-CSOB/Profil-CSOB/Stranky/default.aspx

[32] [online]. [cit. 2014-04-19]. Dostupné z: http://finexpert.e15.cz/profil-csob-dve-banky-v-jedne

[33] [online]. [cit. 2014-04-22]. Dostupné z: http://www.banky.cz/csob

[34] [online]. [cit. 2014-04-22]. Dostupné z: https://www.airbank.cz/cs/vse-o-air-bank/bezpecnost/

[35] [online]. [cit. 2014-04-22]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/servis-24-internetbanking---zabezpeceni-d00014581

[36] [online]. [cit. 2014-04-22]. Dostupné z: http://www.mojebanka.cz/cs/desatero-bezpecnosti.shtml

[37] [online]. [cit. 2014-04-22]. Dostupné z: http://www.csob.cz/cz/Lide/Elektronicke-bankovnictvi/Stranky/CSOB-InternetBanking-24.aspx

[38] [online]. [cit. 2014-04-22]. Dostupné z: http://www.csob.cz/WebCsob/Lide/Elektronicke-bankovnictvi/CSOB_IB24_prirucka_zkrac.pdf

[39] [online]. [cit. 2014-04-26]. Dostupné z: http://www.qualys.com/company/newsroom/news-releases/usa/2010-07-29/

[40] [online]. [cit. 2014-04-26]. Dostupné z: http://www.qualys.com/

[41] [online]. [cit. 2014-04-26]. Dostupné z: https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy

[42] [online]. [cit. 2014-04-26]. Dostupné z: http://www.bezpecnyinternet.cz/o-projektu/

[43] [online]. [cit. 2014-04-26]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/druhy-a-ucel-hesel-d00014572

[44] DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. Vyd. 1. Brno: CP Books, 2005, 50 s. ISBN 80-251-0574-1.

[45] [online]. [cit. 2014-05-01]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

[46] [online]. [cit. 2014-05-01]. Dostupné z: https://www.rb.cz/o-bance/informacni-a-online-sluzby/bezpecnostni-zasady/

[47] [online]. [cit. 2014-05-01]. Dostupné z: http://www.bezpecnyinternet.cz/deti/rady-pro-tebe/desatero-bezpecneho-internetu.aspx

Seznam příloh

Příloha A - Dotazník

Používáte Internetové bankovnictví, a pokud ano, jste s ním spokojeni?

1. Kolik Vám je let?
2. Vaše povolání?
   - ☐ Student
   - ☐ Dělník
   - ☐ Technik
   - ☐ Úředník
   - ☐ Důchodce
3. Vaše nejvyšší dosažené vzdělání?
   - ☐ Základní
   - ☐ Střední odborné bez maturity
   - ☐ Střední odborné s maturitou
   - ☐ Vyšší odborné
   - ☐ Vysokoškolské Bc.
   - ☐ Vysokoškolské Ing., Mgr.
   - ☐ Vysokoškolské vyšší
4. Máte bankovní účet?
   - ☐ ANO
   - ☐ NE
5. Jakou využíváte banku?
6. Používáte Internetové bankovnictví?
   - ☐ ANO
   - ☐ NE
7. Přijde Vám jako jednoduché, dostupné a spolehlivé?
   - ☐ ANO
   - ☐ ČÁSTEČNĚ
   - ☐ NE
   - ☐
8. Jaký typ zabezpečení využíváte? (zaškrtněte i více možností)
   - ☐ Jméno, heslo
   - ☐ Potvrzovací SMS
   - ☐ Certifikát
   - ☐ PIN kalkulátor
   - ☐ Biometrie
   - ☐
9. Přijde Vám způsob zabezpečení dostatečný?
   - ☐ ANO
   - ☐ ČÁSTEČNĚ
   - ☐ NE
   - ☐